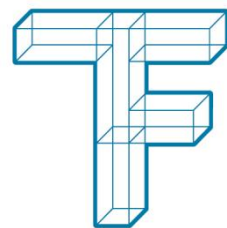




# IPA Dokumentation



TECHNISCHE  
FACHSCHULE  
BERN

**Kunde**  
**Projektname**  
**Autor**  
**Ausgabedatum**  
**Version**

Technische Fachschule Bern - Ressort Informatik  
Zentrales Logmanagement in Betrieb nehmen  
Felix Imobersteg  
27. Februar 2015  
V1.0  
X = Entwurf, in Arbeit – V = Version, freigegeben

**Status**

In Arbeit

In Prüfung

Genehmigt, zur  
Nutzung

☐☒☐

## Beteiligter Personenkreis

Benutzer, Anwender  
Prüfung

Technische Fachschule Bern – Ressort Informatik  
Ivan Cosic  
Nick Tschannen  
Xaver Imboden  
Christina Ernst-Perrone  
Hetem Shaqiri

Genehmigung  
zur Information, Kenntnis



## 1. Dokumentinformationen

### 1.1 Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Name	Beschreibung
X0.1	2013-06-23	A. Mueller	Dokumentvorlage QV2013
X0.2	2015-02-06	F. Imobersteg	Anpassen der Dokumentenvorlage an das TF Bern CI/CD
X0.3	2015-02-09	F. Imobersteg	Zeitplan, Aufgabenstellung, Vorkenntnisse, Vorarbeiten, Firmenstandards, Istzustand, Sollzustand, Vorgehensziele, Systemziele
X0.4	2015-02-10	F. Imobersteg	Anforderungen, Risikoanalyse, Variantenentscheid
X0.5	2015-02-11	F. Imobersteg	Logserver Konzept
X0.6	2015-02-13	F. Imobersteg	Namenskonzept, Monitoring-Konzept, Berechtigungskonzept
X0.7	2015-02-16	F. Imobersteg	Testkonzept, Backupkonzept, ISDS-Konzept
X0.8	2015-02-17	F. Imobersteg	Grundinstallation Logserver, Installation Graylog Server, Installation Graylog Web, Installation Logstash
X0.9	2015-02-18	F. Imobersteg	Backupsript, Postfix, nginx
X0.10	2015-02-20	F. Imobersteg	Installation sendende Hosts
X0.11	2015-02-23	F. Imobersteg	Konfiguration Monitoring, Testing
X0.12	2015-02-24	F. Imobersteg	Management Summary, Glossar, Quellenverzeichnis
X0.13	2015-02-25	F. Imobersteg	Abschlussbericht
V1.0	2015-02-27	F. Imobersteg	Finale Version



## 1.2 Referenzierte Dokumente

Quelle	Beschreibung
<a href="https://redmine.lwb.ch/redmine/projects/ressort-informatik/wiki/Standardinstallation_Linux">https://redmine.lwb.ch/redmine/projects/ressort-informatik/wiki/Standardinstallation_Linux</a>	Zeigt die Standardinstallation von Linux
S:\RESSORT\INF\Dokumentationen\Netzwerk\Netzwerk logisch\Netzwerk_LWB_v06.vsd	Zeigt den logischen Aufbau des TF Bern Netzwerkes
S:\RESSORT\INF\Dokumentationen\Netzwerk\Backup\Backupkonzept.xlsx	Backupkonzept TF Bern
S:\_PROZESSE_LWB\FORMATVORLAGEN\TFB ERN_Dokument_Hoch.dotx	Dokumentenvorlage Hochformat
S:\RESSORT\INF\Dokumentationen\Netzwerk\IP-Konzept\MAN20070529LWB IP Konzept.doc	IP Konzept

## 1.3 Verwendete Abkürzungen

Abkürzung	Bedeutung
ACL	Access Control List
BEWAN	Kantonales Wide Area Network des Kanton Bern
CD	Corporate Design
CI	Corporate Identity
FE	Felsenau
FEB	Felsenau Battage
FEK	Felsenau Kopfbau
GELF	Graylog Extended Log Format
IPA	Individuelle praktische Arbeit
LO	Lorraine
LOH	Lorraine Hauptgebäude
LOS	Lorraine Shed
LWB	Lehrwerkstätten Bern
MA	Mitarbeiter
OdA	Organisation der Arbeitswelt
PPA	Personal Package Archive
QV	Qualifikationsverfahren
REST	Representational State Transfer
RI	Ressort Informatik
TF Bern	Technische Fachschule Bern (Abkürzung nur zur internen Verwendung)
VZ	Verzeichnis
WYSIWYG	What you see is what you get



## 2. Inhaltsverzeichnis

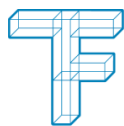
<b>IPA Dokumentation .....</b>	<b>1</b>
<b>1. Dokumentinformationen .....</b>	<b>2</b>
1.1 Änderungskontrolle, Prüfung, Genehmigung .....	2
1.2 Referenzierte Dokumente .....	3
1.3 Verwendete Abkürzungen .....	3
<b>2. Inhaltsverzeichnis .....</b>	<b>4</b>
<b>3. Abbildungsverzeichnis .....</b>	<b>9</b>
<b>4. Tabellenverzeichnis .....</b>	<b>10</b>
<b>5. Hinweise zur Formatierung .....</b>	<b>13</b>
5.1 Konsoleneingabe .....	13
5.2 Textdatei .....	13
<b>6. Management Summary .....</b>	<b>14</b>
6.1 Ausgangssituation .....	14
6.2 Umsetzung .....	14
6.3 Ergebnis .....	14
6.4 Empfehlung für weiteres Vorgehen .....	14
<b>Teil 1: Ablauf und Umfeld .....</b>	<b>15</b>
<b>7. Aufgabenstellung .....</b>	<b>16</b>
7.1 Ausgangslage .....	16
7.2 Auftragsformulierung .....	16
7.3 Mittel und Methoden .....	17
7.4 Projektorganigramm .....	18
7.5 Projektrollen .....	19
<b>8. Vorkenntnisse .....</b>	<b>20</b>
<b>9. Vorarbeiten .....</b>	<b>21</b>
<b>10. Firmenstandards .....</b>	<b>22</b>
<b>11. Organisation der IPA .....</b>	<b>23</b>
11.1 Dokumentenablage .....	23
11.2 Arbeitsplatz .....	24
11.3 Datensicherung der IPA .....	24
<b>12. Zeitplan .....</b>	<b>25</b>
12.1 Meilensteine .....	27
<b>13. Arbeitsjournal .....</b>	<b>28</b>
13.1 Erster Tag: Montag, 09. Februar 2015 .....	28
13.2 Zweiter Tag: Dienstag, 10. Februar 2015 .....	30
13.3 Dritter Tag: Mittwoch, 11. Februar 2015 (halber Tag) .....	31
13.4 Vierter Tag: Freitag, 13. Februar 2015 .....	32
13.5 Fünfter Tag: Montag, 16. Februar 2015 .....	33
13.6 Sechster Tag: Dienstag, 17. Februar 2015 .....	35
13.7 Siebter Tag: Mittwoch, 18. Februar 2015 (halber Tag) .....	36
13.8 Achter Tag: Freitag, 20. Februar 2015 .....	37
13.9 Neunter Tag: Montag, 23. Februar 2015 .....	38
13.10 Zehnter Tag: Dienstag, 24. Februar 2015 .....	39
13.11 Elfter Tag: Mittwoch, 25. Februar 2015 (halber Tag) .....	40
13.12 Zwölfter Tag: Freitag, 27. Februar 2015 (halber Tag) .....	41
13.13 Arbeitszeit total .....	42
<b>14. Abschlussbericht .....</b>	<b>43</b>
14.1 Vergleich Ist/Soll .....	43
14.2 Mittelbedarf .....	43
14.3 Realisierungsbericht .....	43
14.4 Testbericht .....	43



14.5	Fazit zum Projekt .....	44
14.6	Persönliches Fazit.....	44
<b>15.</b>	<b>Unterschriften Teil 1 .....</b>	<b>45</b>
<b>Teil 2:</b>	<b> Projektdokumentation .....</b>	<b>46</b>
<b>16.</b>	<b> Projektmethode .....</b>	<b>47</b>
16.1	Erläuterung der Phasen .....	47
16.1.1	Initialisierung.....	47
16.1.2	Konzept .....	47
16.1.3	Realisierung.....	47
16.1.4	Einführung .....	47
<b>17.</b>	<b>Initialisierung.....</b>	<b>48</b>
17.1	Studie Ist-Zustand / Soll-Zustand .....	48
17.1.1	Istzustand .....	48
17.1.2	Sollzustand .....	48
17.2	Vorgehensziele .....	50
17.3	Systemziele.....	51
17.4	Anforderungen .....	51
17.4.1	Funktionale Anforderungen .....	51
17.4.2	Nicht funktionale Anforderungen .....	53
17.5	Risikoanalyse .....	54
17.5.1	Legende.....	55
17.6	Risikograph .....	56
17.6.1	Vor Massnahmen .....	56
17.6.2	Nach Massnahmen.....	57
<b>18.</b>	<b>Konzept.....</b>	<b>58</b>
18.1	Logserver Konzept.....	58
18.1.1	Systemarchitektur.....	58
18.1.2	Erläuterung der verwendeten Dienste .....	59
18.1.3	Erläuterung der verwendeten Protokolle .....	60
18.1.4	Service Schnittstellen .....	61
18.1.5	Netzwerk Konfiguration Logserver .....	61
18.1.6	Netzübergreifende Kommunikation .....	61
18.1.7	Systemanforderungen VMLOG1 .....	62
18.1.8	Inputs Logstash .....	62
18.1.9	Inputs Graylog .....	63
18.1.10	Filter Logstash .....	63
18.1.11	Extractor Graylog.....	63
18.1.12	Outputs Logstash .....	63
18.1.13	Outputs Graylog .....	63
18.1.14	Graylog Streams.....	64
18.1.15	Graylog Alerts .....	64
18.1.16	Logversand .....	65
18.1.17	Installationsscript .....	65
18.1.18	Dashboards .....	66
18.1.19	Grundinstallation VMLOG1 .....	66
18.1.20	Zu installierende Software (VMLOG1) .....	66
18.1.21	Zugriff Logserver .....	67
18.2	Namenskonzept .....	67
18.2.1	Server .....	67



18.2.2	Netzwerkkomponenten .....	69
18.3	Monitoring-Konzept .....	70
18.3.1	Checks VMLOG1 .....	70
18.3.2	Checks sendende Windows Server .....	71
18.3.3	Checks sendende Linux Server .....	71
18.3.4	Checks sendende Netzwerkkomponenten .....	71
18.3.5	Alarmierung .....	71
18.4	Berechtigungskonzept .....	72
18.4.1	Konfiguration in Graylog .....	72
18.4.2	Testbenutzer .....	72
18.4.3	Mitglieder G_MA-IMF .....	72
18.4.4	Physikalischer Zugriff (Serverraum) .....	72
18.5	Backupkonzept .....	72
18.5.1	Art des Backups .....	73
18.5.2	Ziel .....	73
18.5.3	Zu sichernde Daten .....	73
18.5.4	Backupjobs .....	73
18.5.5	Aufbewahrungsdauer .....	73
18.5.6	Backuptyp .....	73
18.5.7	Benachrichtigung .....	74
18.5.8	Verschlüsselung des Backups .....	74
18.5.9	Restore .....	74
18.6	ISDS Konzept .....	74
18.6.1	Zugriff auf das TF Bern Netzwerk .....	74
18.6.2	Zugriff auf lokale Computer .....	74
18.6.3	IPA Daten .....	74
18.6.4	Virenschutz .....	75
18.6.5	Internetschutz .....	75
18.6.6	Übertragung von Daten .....	75
18.7	Testkonzept .....	75
18.7.1	Testobjekte .....	75
18.7.2	Testkategorien .....	76
18.7.3	Testarten .....	76
18.7.4	Testvoraussetzungen .....	76
18.7.5	Testvorgehen .....	76
18.7.6	Testaccounts .....	76
18.7.7	Vorlage Testfälle .....	77
18.7.8	Fehlerprotokoll .....	77
18.7.9	Vorlage Fehlerprotokoll .....	77
18.7.10	Testabnahme .....	77
18.7.11	Funktionelle Anwendertests .....	78
18.7.12	Nicht funktionale Anwendertests .....	82
18.7.13	Sicherheitstest .....	82
<b>19.</b>	<b>Realisierung .....</b>	<b>84</b>
19.1	Grundinstallation VMLOG1 .....	84
19.1.1	Verbindung zum vCenter .....	84
19.1.2	Erstellen der VM .....	84
19.1.3	Debian Installation .....	85
19.1.4	Netzwerkconfiguration .....	87



19.1.5	Updaten des Systems .....	87
19.1.6	Installation VMWare Tools .....	88
19.1.7	Festplatte mounten .....	89
19.1.8	Logonscreen .....	90
19.1.9	Willkommensscreen .....	90
19.1.10	DNS Einträge .....	91
19.2	Installation Java .....	92
19.3	Installation MongoDB .....	92
19.4	Installation Elasticsearch .....	93
19.5	Graylog Server Installation .....	94
19.6	Graylog Web .....	96
19.7	Graylog Input Konfiguration .....	96
19.8	Graylog LDAP Konfiguration .....	97
19.9	Logstash Installation .....	98
19.10	Logstash Linux Input Konfiguration .....	99
19.11	Logstash Windows Input Konfiguration .....	99
19.12	Logstash Cisco Input Konfiguration .....	100
19.13	Logstash Linux Syslog Filter Konfiguration .....	100
19.14	Logstash Windows Eventlog Filter Konfiguration .....	100
19.15	Logstash Cisco Syslog Filter Konfiguration .....	101
19.16	Logstash Graylog Output Konfiguration .....	101
19.17	Logstash Forwarder Paket erstellen .....	101
19.19	Graylog Stream Konfiguration .....	104
19.20	Graylog Alert Konfiguration .....	105
19.21	Backup .....	105
19.21.1	Ausführen eines manuelles Backups .....	107
19.21.2	Anzeige des Backupstatus .....	108
19.21.3	Anzeige des Backupinhalts .....	108
19.21.4	Restore einer Datei oder eines Ordners .....	108
19.22	Installation Postfix .....	108
19.23	nginx Reverse Proxy .....	109
19.24	Test VM's .....	110
19.24.1	Vagrantfile Debian Wheezy .....	110
19.24.2	Vagrantfile Windows Server 2008R2 .....	111
19.24.3	Vagrantfile Windows Server 2012 .....	111
19.25	Installation sendende Windows Server .....	112
19.26	Installation sendende Linux Server .....	112
19.27	Konfiguration sendende Cisco Switches .....	113
19.28	Installation Logclient (VMLOG1) .....	113
19.29	Konfiguration Icinga .....	114
19.29.1	Hostgruppe Logserver .....	115
19.29.2	Host VMLOG1 .....	115
19.29.3	Serviceobjekte VMLOG1 .....	115
19.29.4	Checks sendende Windows Server .....	116
19.29.5	Checks sendende Linux Server .....	117
19.29.6	Abschluss der Konfiguration .....	118
19.30	Aufgetretene Probleme .....	118
19.30.1	MongoDB: Connection Refused .....	118
19.30.2	Graylog-Server: Startet nicht .....	119
19.30.3	Kein funktionierendes Debian-Paket für Logstash Forwarder vorhanden .....	119
19.30.4	Kein Logempfang von Cisco Routern .....	120
19.31	Testprotokoll .....	120



19.31.1	Funktionelle Anwendertests .....	120
19.31.2	Nicht funktionale Anwendertests .....	126
19.31.3	Sicherheitstest .....	127
19.31.4	Fehlerprotokolle .....	128
19.31.5	Testabnahme .....	129
<b>20.</b>	<b>Quellenverzeichnis .....</b>	<b>130</b>
<b>21.</b>	<b>Glossar .....</b>	<b>131</b>
<b>22.</b>	<b>Unterschriften für Abnahme .....</b>	<b>132</b>
<b>Teil 3: Anhang .....</b>		<b>133</b>
<b>23.</b>	<b>Backupkonzept .....</b>	<b>134</b>
<b>24.</b>	<b>Standardinstallation Linux .....</b>	<b>135</b>
24.1	Step by Step Debian Installation .....	135
<b>25.</b>	<b>IP Konzept .....</b>	<b>136</b>
25.1	Lorraine .....	136
25.2	Felsenau .....	136
25.3	Detaillierte Einteilungen Lorraine .....	136
25.3.1	Verwaltung .....	136
25.3.2	Lehrer .....	137
25.3.3	Unterricht .....	137
25.3.4	VoIP .....	137
25.3.5	Service .....	137
25.3.6	Default .....	138
25.3.7	MGNT .....	138
25.3.8	ELAN .....	138
25.4	Detaillierte Einteilungen Felsenau .....	138
25.4.1	Verwaltung .....	138
25.4.2	Lehrer .....	139
25.4.3	Unterricht .....	139
25.4.4	VoIP .....	139
25.4.5	Service .....	139
25.4.6	Default .....	140
25.4.7	MGNT .....	140
25.4.8	ELAN .....	140





### 3. Abbildungsverzeichnis

Abbildung 1: Projektorganigramm .....	18
Abbildung 2: Ordnerstruktur - Dokumentenablage .....	23
Abbildung 3: Arbeitsplatz .....	24
Abbildung 4: Hermes 5 IPA .....	47
Abbildung 5: Systemarchitektur .....	58
Abbildung 6: Graylog Dashboard .....	66
Abbildung 7: Symbol VM erstellen .....	84
Abbildung 8: Soll - VM erstellen .....	85
Abbildung 9: Softwareauswahl - Debian Installer .....	86
Abbildung 10: VMware Tools Status .....	88
Abbildung 11: Erwartetes Ergebnis .....	97
Abbildung 12: Graylog LDAP: Serverkonfiguration .....	97
Abbildung 13: Graylog LDAP: Erweiterte Konfiguration .....	98
Abbildung 14: Graylog Stream Konfiguration .....	104
Abbildung 15: TF1 Screenshot .....	120
Abbildung 16: TF2 Screenshot .....	121
Abbildung 17: TF3 Screenshot .....	122
Abbildung 18: TF4 Screenshot .....	122
Abbildung 19: TF6 Screenshot .....	123
Abbildung 20: TF9 Screenshot .....	125
Abbildung 21: TF10 Screenshot .....	126
Abbildung 22: TF11 Screenshot .....	126
Abbildung 23: TF12 Screenshot .....	127
Abbildung 24: TF14 Screenshot .....	128



## 4. Tabellenverzeichnis

Tabelle 1: Projektrollen.....	19
Tabelle 2: Vorkenntnisse.....	20
Tabelle 3: Vorarbeiten.....	21
Tabelle 4: Firmenstandards.....	22
Tabelle 5: Backupkonzept - VMFSV1.....	24
Tabelle 6: Zeitplan - Teil 1.....	25
Tabelle 7: Zeitplan - Teil 2.....	26
Tabelle 8: Zeitplan.....	27
Tabelle 9: Arbeitsjournal: Montag, 09. Februar 2015.....	30
Tabelle 10: Arbeitsjournal: Dienstag, 10. Februar 2015.....	31
Tabelle 11: Arbeitsjournal: Mittwoch, 11. Februar 2015 (halber Tag).....	32
Tabelle 12: Arbeitsjournal: Freitag, 13. Februar 2015.....	33
Tabelle 13: Arbeitsjournal: Montag, 16. Februar 2015.....	34
Tabelle 14: Arbeitsjournal: Dienstag, 17. Februar 2015.....	36
Tabelle 15: Arbeitsjournal: Mittwoch, 18. Februar 2015 (halber Tag).....	37
Tabelle 16: Arbeitsjournal: Freitag, 20. Februar 2015.....	38
Tabelle 17: Arbeitsjournal: Montag, 23. Februar 2015.....	39
Tabelle 18: Arbeitsjournal: Dienstag, 24. Februar 2015.....	40
Tabelle 19: Arbeitsjournal: Mittwoch, 25. Februar 2015 (halber Tag).....	41
Tabelle 20: Arbeitsjournal: Freitag, 27. Februar 2015 (halber Tag).....	41
Tabelle 21: Arbeitszeit total.....	42
Tabelle 22: Unterschriften Teil 1.....	45
Tabelle 23: Vorgehensziele.....	50
Tabelle 24: Systemziele.....	51
Tabelle 25: Funktionale Anforderungen.....	53
Tabelle 26: Nicht funktionale Anforderungen.....	53
Tabelle 27: Risikoanalyse.....	54
Tabelle 28: Schadensausmass.....	55
Tabelle 29: Eintrittswahrscheinlichkeit.....	55
Tabelle 30: Risikograph - vor Massnahmen.....	56
Tabelle 31: Risikograph - nach Massnahmen.....	57
Tabelle 32: Erläuterung der verwendeten Dienste.....	59
Tabelle 33: Erläuterung der verwendeten Protokolle.....	60
Tabelle 34: Service Schnittstellen.....	61
Tabelle 35: Netzwerk Konfiguration VMLOG1.....	61
Tabelle 36: Systemanforderungen VMLOG1.....	62
Tabelle 37: Inputs Logstash.....	62
Tabelle 38: Inputs Graylog.....	63
Tabelle 39: Outputs Logstash.....	63
Tabelle 40: Graylog Streams.....	64
Tabelle 41: Graylog Alerts.....	64
Tabelle 42: Logversand - Linux Server.....	65
Tabelle 43: Logversand - Windows Server.....	65
Tabelle 44: Logversand - Switches und Router.....	65
Tabelle 45: Zu installierende Software (VMLOG1).....	67
Tabelle 46: Namenskonzept - Server -Typ.....	68
Tabelle 47: Namenskonzept - Server - Zweck.....	68
Tabelle 48: Namenskonzept - Server - Beispiele.....	68
Tabelle 49: Namenskonzept - Netzwerkkomponenten - Standort.....	69
Tabelle 50: Namenskonzept - Netzwerkkomponenten - Stockwerk.....	69
Tabelle 51: Namenskonzept - Netzwerkkomponenten - Typ.....	69
Tabelle 52: Namenskonzept - Netzwerkkomponenten - Beispiele.....	70
Tabelle 53: Monitoring-Konzept - Checks VMLOG1.....	71
Tabelle 54: Monitoring-Konzept - Checks sendende Windows Server.....	71
Tabelle 55: Monitoring-Konzept - Checks sendende Linux Server.....	71
Tabelle 56: Mitglieder G_MA-IMF.....	72



Tabelle 57: Zu sichernde Daten .....	73
Tabelle 58: Testobjekte .....	75
Tabelle 59: Testarten .....	76
Tabelle 60: Vorlage Testfälle.....	77
Tabelle 61: Vorlage Fehlerprotokoll .....	77
Tabelle 62: Testfall TF1 (Zugriff Graylog Web funktioniert) .....	78
Tabelle 63: Testfall TF2 (Installationsscript Windows Server 2008R2 funktioniert).....	78
Tabelle 64: Testfall TF3 (Installationsscript Windows Server 2012 funktioniert) .....	78
Tabelle 65: Testfall TF4 (Installationsscript Linux Server funktioniert) .....	79
Tabelle 66: Testfall TF5 (Backup funktioniert) .....	79
Tabelle 67: Testfall TF6 (Sendende Linux Server hinzugefügt).....	79
Tabelle 68: Testfall TF7 (Sendende Windows Server hinzugefügt).....	80
Tabelle 69: Testfall TF8 (Sendende Netzwerkkomponenten hinzugefügt) .....	80
Tabelle 70: Testfall TF9 (Monitoring VMLOG1 ersichtlich) .....	80
Tabelle 71: Testfall TF10 (Graylog Streams eingerichtet) .....	81
Tabelle 72: Testfall TF11 (Graylog Übersichtsdashboard eingerichtet).....	81
Tabelle 73: Testfall TF12 (Schneller Zugriff auf Webinterface) .....	82
Tabelle 74: Testfall TF13 (Anmeldung für Mitglieder G_MA-INF).....	82
Tabelle 75: Testfall TF14 (Anmeldung für Nicht-Mitglieder G_MA-INF) .....	82
Tabelle 76: Testfall TF15 (Anmeldung für Nicht-Mitglieder G_MA-INF) .....	83
Tabelle 77: vCenter Login .....	84
Tabelle 78: Logonscreen (Soll) .....	90
Tabelle 79: Willkommensbildschirm (Soll) .....	91
Tabelle 80: DNS Einträge Logserver .....	91
Tabelle 81: Icinga Graylog Benutzer .....	114
Tabelle 82: Testfall TF1 (Zugriff Graylog Web funktioniert) .....	120
Tabelle 83: Testfall TF2 (Installationsscript Windows Server 2008R2 funktioniert).....	121
Tabelle 84: Testfall TF3 (Installationsscript Windows Server 2012 funktioniert) .....	122
Tabelle 85: Testfall TF4 (Installationsscript Linux Server funktioniert) .....	122
Tabelle 86: Testfall TF5 (Backup funktioniert) .....	123
Tabelle 87: Testfall TF6 (Sendende Linux Server hinzugefügt).....	123
Tabelle 88: Testfall TF7 (Sendende Windows Server hinzugefügt).....	124
Tabelle 89: Testfall TF8 (Sendende Netzwerkkomponenten hinzugefügt) .....	124
Tabelle 90: Testfall TF9 (Monitoring VMLOG1 ersichtlich) .....	125
Tabelle 91: Testfall TF10 (Graylog Streams eingerichtet) .....	126
Tabelle 92: Testfall TF11 (Graylog Übersichtsdashboard eingerichtet).....	126
Tabelle 93: Testfall TF12 (Schneller Zugriff auf Webinterface) .....	127
Tabelle 94: Testfall TF13 (Anmeldung für Mitglieder G_MA-INF).....	127
Tabelle 95: Testfall TF14 (Anmeldung für Nicht-Mitglieder G_MA-INF) .....	128
Tabelle 96: Testfall TF15 (Anmeldung für Nicht-Mitglieder G_MA-INF) .....	128
Tabelle 97: Fehlerprotokoll 1 .....	128
Tabelle 98: Testabnahme.....	129
Tabelle 99: Quellenverzeichnis .....	130
Tabelle 100: Glossar .....	131
Tabelle 101: Unterschriften für Abnahme .....	132
Tabelle 102: Backupkonzept .....	134
Tabelle 103: Angaben Standardinstallation Linux .....	135
Tabelle 104: Netze Lorraine .....	136
Tabelle 105: Netze Felsenau .....	136
Tabelle 106: Netz - Verwaltung Lorraine.....	136
Tabelle 107: Netz - Lehrer Lorraine .....	137
Tabelle 108: Netz - Unterricht Lorraine .....	137
Tabelle 109: Netz - VoIP Lorraine .....	137
Tabelle 110: Netz - Service Lorraine.....	137
Tabelle 111: Netz - Default Lorraine .....	138
Tabelle 112: Netz - MGNT Lorraine .....	138
Tabelle 113: Netz - ELAN Lorraine .....	138
Tabelle 114: Netz - Verwaltung Felsenau .....	138
Tabelle 115 Netz - Lehrer Felsenau .....	139



---

Tabelle 116 Netz - Unterricht Felsenau .....	139
Tabelle 117 Netz - VoIP Felsenau .....	139
Tabelle 118 Netz - Service Felsenau .....	139
Tabelle 119 Netz - Default Felsenau .....	140
Tabelle 120 Netz - MGNT Felsenau .....	140
Tabelle 121 Netz - ELAN Felsenau .....	140



## 5. Hinweise zur Formatierung

Nachfolgend sind Beispiele zur Formatierung dieses Dokuments aufgeführt.

### 5.1 Konsoleneingabe

Die nachfolgende Darstellung stellt eine Kommandozeileneingabe dar:

```
root@VMLOG1:~# nano /etc/hosts
```

### 5.2 Textdatei

Die nachfolgende Formatierung stellt den Inhalt einer Textdatei dar. Der Dateiname ist in der vorhergehenden Kommandozeileneingabe oder im Beschrieb ersichtlich.

```
127.0.0.1    localhost
86.118.120.30 VMLOG1.lwb.ch  VMLOG1

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

## 6. Management Summary

### 6.1 Ausgangssituation

Bisher wurden in der Technischen Fachschule Bern keine Logs zentral gesammelt. Jeder Server, Switch oder Router speichert seine Logs lokal. Zur Auswertung muss sich ein MA des RI auf dem jeweiligen Host anmelden und die Einträge mühsam durchsuchen. Die Möglichkeiten der Bordmittel sind stark eingeschränkt. Besonders wenn dies im Störfall auf mehreren unterschiedlichen Geräten wiederholt werden muss, geht viel wertvolle Zeit verloren.

Weiter war es bisher nicht möglich, Daten über einen Zeitverlauf darzustellen. Dies ist jedoch zur proaktiven Auswertung zwingend notwendig.

### 6.2 Umsetzung

Im Rahmen dieser IPA wurde ein Server zur Verwaltung der Logs eingerichtet. Die komplette Installation basiert auf frei verfügbaren Open Source Produkten. Auf diese Weise entstehen keine Lizenzkosten und der Motion des Berner Grossrats „2013.0783 „Synergien beim Software-Einsatz im Kanton Bern nutzen“ wird Rechnung getragen.

Das gesamte Projekt wurde mit der Projektmethode Hermes 5 IPA geplant und umgesetzt. In diesem Dokument sind sämtliche Phasen ersichtlich. Weiter sind alle Informationen, welche das RI zum Betrieb der Log-Infrastruktur benötigt, ersichtlich.

Die Konfiguration der sendenden Geräte wurde ebenfalls abgeschlossen.

### 6.3 Ergebnis

Der zentrale Server zur Verwaltung der Logs wurde erfolgreich in Betrieb genommen. Die Lognormalisierung wurde für die Systemlogs aller Geräte eingerichtet. Alle Switches, Linux und Windows Server senden wie gewünscht die Systemlogs an den Logserver. Die beiden Router wurden nicht im Rahmen dieses Projekts konfiguriert, da Einschränkungen für den laufenden Schulbetrieb nicht hätten ausgeschlossen werden.

Das Zugriffskonzept wurde ausgearbeitet und umgesetzt. Ein Zugriff auf das Graylog Webinterface (<https://log.lwb.ch>) ist für MA des RI über ihren gewohnten Domänenbenutzer möglich.

### 6.4 Empfehlung für weiteres Vorgehen

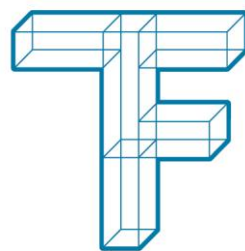
Es wird empfohlen, auch auf den restlichen Hosts den Logversand soweit als möglich einzurichten. Weiter wurden bei der Installation mehrere Auffälligkeiten auf einzelnen Server entdeckt, welche von den verantwortlichen Personen genauer angeschaut werden sollte.



## Teil 1: Ablauf und Umfeld

**IPA Projektname:**  
**Autor:**

Zentrales Logmanagement in Betrieb nehmen  
Felix Imobersteg



TECHNISCHE  
FACHSCHULE  
BERN



## 7. Aufgabenstellung

### 7.1 Ausgangslage

Aufgrund der gewachsenen Anzahl von Netzwerkkomponenten und Server wird die Einführung eines Logmanagement Systems angestrebt. Zurzeit wird kein Logmanagement Dienst in der Technischen Fachschule Bern eingesetzt. Aktuell ist das Auswerten der Logs im Problemfall über mehrere Hosts zeitaufwändig und mühsam.

### 7.2 Auftragsformulierung

- Konfiguration der Software und Dienste
  - Installation von Linux Debian 7 Server in der produktiven Umgebung
    - Grundinstallation des Linux Servers
    - Sämtliche Konfigurationen, die nicht dem Standard entsprechen, werden mithilfe eines Skripts gesichert.
    - Konfiguration des Servers nach TF Bern Standard
    - Erfassen im Monitoring analog zum Server VMWEB1 (Systemdienste) und zusätzlich Logmanagement Dienste (Icinga)
- Installation von Graylog2 (aktuellste Version) auf dem Server (sämtliche Dienste sollen auf einem Server installiert werden)
  - Installation und Konfiguration von Graylog2 Server
  - Installation und Konfiguration von Graylog2 Webserver
  - Installation und Konfiguration von Elasticsearch
  - Installation und Konfiguration von MongoDB
  - Installation und Konfiguration von Logstash zur grundlegenden Normalisierung und Weiterleitung von Logs
  - Installation und Konfiguration von nginx zur Verwendung als Reverse Proxy, um den Zugriff auf das Graylog Webinterface über HTTPS zu ermöglichen
- Einrichten der sendenden Server und Netzwerkkomponenten auf allen Hosts (siehe Mittel und Methoden)
  - Installation benötigter Dienste auf allen sendenden Hosts (NXLog, Logstash-Forwarder)
  - Konfiguration des Logversands auf allen sendenden Hosts
  - Die Installation und Konfiguration wird zur Automatisierung mithilfe eines eigenständig erstellten Skripts durchgeführt
- Alle nachfolgende Hosts im Graylog2 erfassen
  - 15 Windows Server (2008 R2 und 2012)
  - 3 Linux Server (Debian 7)
  - 33 Cisco Switches und Router
- Definieren der Daten zum Loggen
  - Windows EventLog
  - Kernel Logs und Local Syslog (Linux)
  - Syslog (Cisco Catalyst)
- Einrichten von Streams zur praktischen Auswertung der von Graylog2 empfangenen Logs
  - Definieren von Streams für DFSR und Windows Eventlogs
  - Definieren von Streams für Logs von Linux Server
  - Definieren von Streams für Logs von Cisco Catalyst Geräten





- Einrichten von Alarming im Graylog2
  - Definieren von drei Alarmtriggern zu Beispiel und Demozwecken
  - Weitere Alarmings werden nicht erfasst, da weitere Alarmings hauptsächlich für Applikationsspezifische Logs sinnvoll sind und diese nicht im Umfang der IPA enthalten sind

### 7.3 Mittel und Methoden

Zur Verfügung stehende Infrastruktur:

- Produktive Server- und Netzwerkumgebung
- VMWare Cluster (2 ESX Server 5.1 mit vSphere 5.5)
- 15 Windows Server (2008 R2 und 2012)
- 3 Linux Server (Debian 7)
- 33 Cisco Switches und Router

Projektmethode:

- Dokumentation nach Hermes 5 IPA

Vorgehen um Projekt gemäss Organisationslehre:

- Systemdenken (Grob, Detail)
- Problemlösungsprozess (IST, SOLL)
- Einhalten der Firmenstandards

Zu verwendende Software:

- Linux Debian 7
- Graylog2 Server
- Graylog2 Webserver
- Elasticsearch
- MongoDB
- Logstash
- Logstash-Forwarder
- NXLog

## 7.4 Projektorganigramm

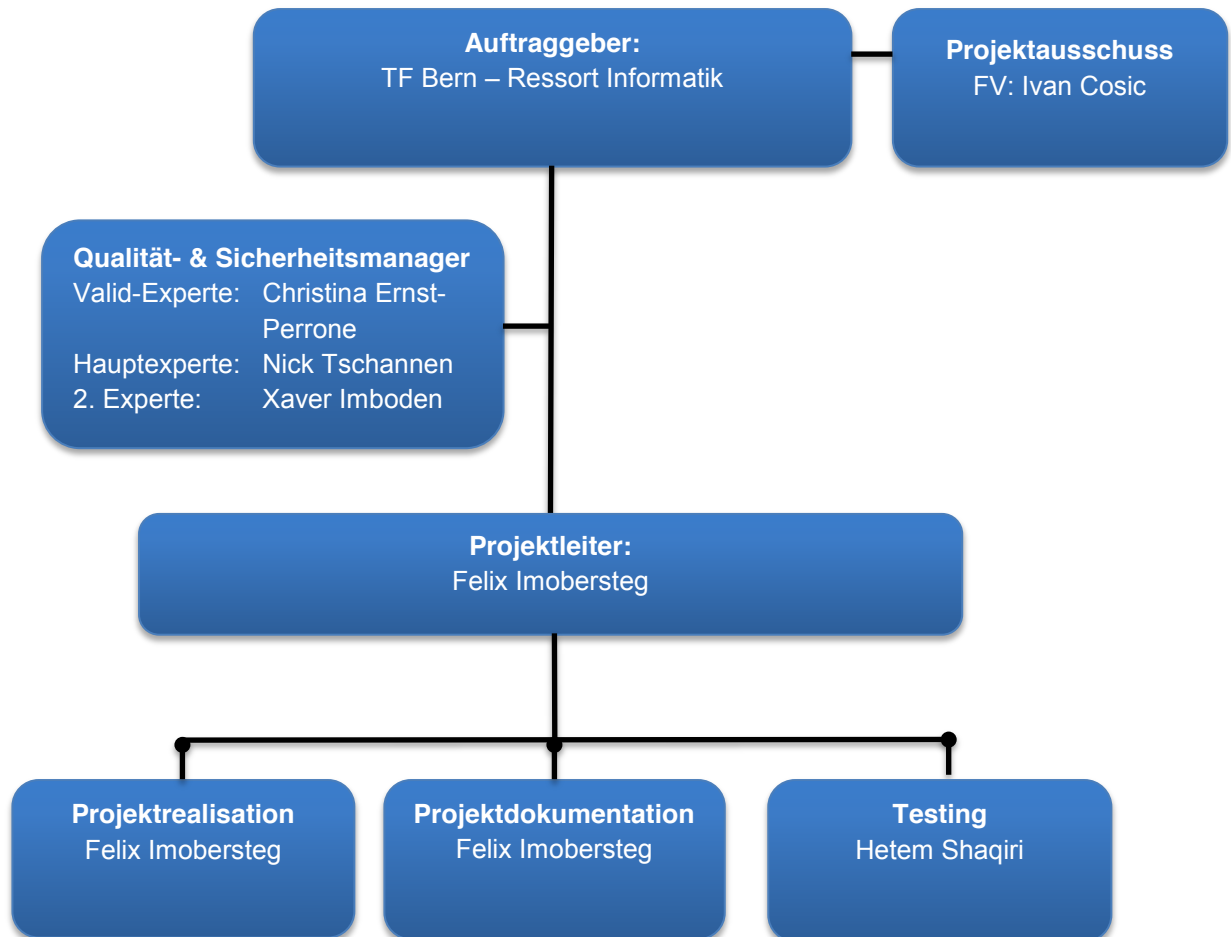


Abbildung 1: Projektorganigramm



## 7.5 Projektrollen

Rolle:	Beschreibung:
<b>Auftraggeber</b> TF Bern – Ressort Informatik	Der Auftraggeber dieses Projekts ist das Ressort Informatik der Technischen Fachschule Bern.
<b>Projektausschuss</b> Ivan Cosic	Die Rolle des Projektausschusses übernimmt der Fachvorgesetzte Ivan Cosic.
<b>Qualität- &amp; Sicherheitsmanager</b> Valid-Experte: Christina Ernst-Perrone Hauptexperte: Nick Tschannen 2. Experte: Xaver Imboden	Die Rolle der Qualität- & Sicherheitsmanager wird durch das IPA-Expertenteam übernommen. Namentlich sind dies: Christina Ernst-Perrone, Nick Tschannen und Xaver Imboden.
<b>Projektleiter</b> Felix Imobersteg	Die Projektleitung liegt bei Felix Imobersteg.
<b>Projektrealisation</b> Felix Imobersteg	Die Projektrealisation wird durch Felix Imobersteg durchgeführt.
<b>Projektdokumentation</b> Felix Imobersteg	Die Projektdokumentation wird durch Felix Imobersteg erstellt.
<b>Testing</b> Hetem Shaqiri	Die Testing wird durch Hetem Shaqiri durchgeführt.

Tabelle 1: Projektrollen



## 8. Vorkenntnisse

Bereich	Erfahrung/Beschrieb
Windows Server 2008R2, 2012	In der TF Bern hatte ich bereits mehrfach die Gelegenheit, einen Windows Server 2008R2 oder 2012 in Betrieb zu nehmen, sowie damit zu arbeiten. Weiter hatte ich im Basislehrjahr und in der Gewerbeschule zu Übungszwecken damit gearbeitet.
Installation und Konfiguration von Hardwarebauteilen	Ich habe bereits diverse Hardwarebauteile installiert und konfiguriert.
Firmenspezifische Standards	Die in den TF Bern geltenden firmenspezifischen Standards sind mir durch die mehrjährige Arbeit bekannt.
Active Directory + DNS	In den TF Bern habe ich das, heute produktiv verwendete, AD und DNS System in Betrieb genommen. Zudem arbeite ich regelmässig damit.
Windows 7	Mit dem Windows 7 Betriebssystem bin ich vertraut.
VMWare	In der TF Bern, wie auch in der Schule, habe ich schon mit Windows Server 2012 gearbeitet.
Linux	Ich habe bereits mehrere produktive Linuxserver in Betrieb genommen. Weiter habe ich Erfahrung mit Linux Desktop Betriebssystemen.
Firewall Konfiguration	Ich nehme regelmässig Konfigurationsanpassungen an der Corporate FW vor.
Routing / Subnetting	Ich bin für das Netzwerk der TF Bern verantwortlich und habe somit Erfahrung mit Routing und Subnetting.
VLAN	Die Theorie und Praxis von VLAN's sind mir geläufig.
Monitoring (Icinga)	Ich habe das Monitoring System in der TF Bern in Betrieb genommen.
Installation Webserver (Apache / nginx)	Ich habe bereits mehrere produktive Webserver in Betrieb genommen.
Switch Konfiguration (Cisco)	Die Konfiguration von Switches ist mir vertraut.

Tabelle 2: Vorkenntnisse



## 9. Vorarbeiten

Die nachfolgenden Vorarbeiten wurden bereits vor dem Start der eigentlichen IPA durchgeführt.

Vorarbeit	Umfang/Beschrieb
Selbststudium	Im Vorfeld der IPA habe ich mir, im Rahmen eines Selbststudiums, Wissen über zentrales Logmanagement, Graylog und Logstash angeeignet.
Informationen bereitstellen	Einige der im Selbststudium gewonnen Informationen habe ich als Notiz festgehalten, um sie während der IPA Umsetzung verwenden zu können.
Vorbereiten der Dokumentationsvorlage	Vor der IPA habe ich die Dokumentationsvorlage von PkOrg an unser Corporate Design angepasst. Weiter habe ich eine Designvorlage für den Zeitplan erstellt.

**Tabelle 3: Vorarbeiten**



## 10. Firmenstandards

Die nachfolgende Tabelle zeigt Firmenstandards, welche bei der IPA Verwendung finden.

Standard	Beschrieb
Namenskonvention	Für die Benutzer, Gruppen und Computer gelten die Namenskonventionen der TF Bern. Diese sind unter dem Kapitel Namenkonzept (Seite 67) ersichtlich.
Dokumentvorlage	Die PkOrg-Dokumentvorlage wurde gemäss der TF Bern Dokumentenvorlage angepasst. (Kopf- und Fusszeile sowie Schriftart und Grösse).
Backup	Die Datensicherung erfolgt nach dem TF Bern Backupkonzept.
Standardinstallation Linux	Die Installation der Linux Server muss gemäss den „Standardinstallation Linux“ der TF Bern durchgeführt werden.
IP Konzept	IP Adressen werden gemäss dem IP Konzept vergeben.

**Tabelle 4: Firmenstandards**

Zu sämtlichen oben aufgeführten Firmenstandards, sind die offiziellen Richtlinien im Anhang beigelegt. Aufgrund der kürzlich durchgeführten Migration sind noch nicht alle Dokumente dem heutigen Standard angepasst. Aus diesem Grund wurden nur die Dokumente beigelegt, welche dem heute gültigen Stand entsprechen.

## 11. Organisation der IPA

### 11.1 Dokumentenablage

Sämtliche Dokumente der IPA werden auf dem Home Laufwerk unter „N:\IPA\Dokumente“ abgelegt. Für jeden Tag wird eine neue Version erstellt und im Unterordner mit dem jeweiligen Datum abgelegt.

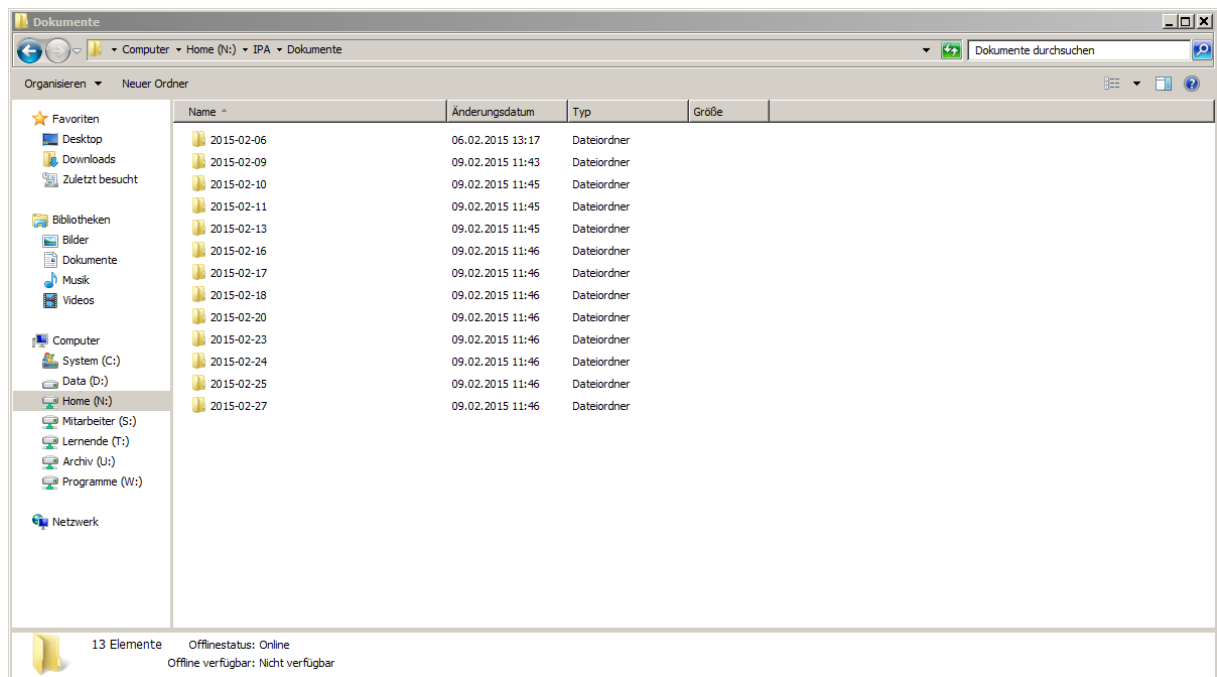


Abbildung 2: Ordnerstruktur - Dokumentenablage

## 11.2 Arbeitsplatz

Der Durchführungsort bzw. Arbeitsplatz der IPA ist mein gewohnter Arbeitsplatz. Dieser befindet sich im Zimmer LOH001 in der Technischen Fachschule Bern - Standort Lorraine.



Abbildung 3: Arbeitsplatz

## 11.3 Datensicherung der IPA

Wie bereits erwähnt, wird pro IPA Tag eine neue Version angelegt und separat gespeichert. Auf diese Weise ist es möglich, schnell auf eine ältere Version zurückzugreifen.

Weiter werden die folgenden Backups gemäss unserem Backupkonzept durchgeführt, um im Notfall darauf zurückgreifen zu können.

Backup	Art	Aufbewahrungsdauer
Tagesbackup	Inkrementell	7 Tage
Wochenbackup	Full	1 Monat
Monatsbackup	Full	1 Jahr
Jahresbackup	Full	10 Jahre

Tabelle 5: Backupkonzept - VMFSV1



## 12. Zeitplan

Tätigkeiten		Sollzeit in Stunden	Istzeit in Stunden	09.02.15 Morgen	09.02.15 Nachmittag	10.02.15 Morgen	10.02.15 Nachmittag	11.02.15 Nachmittag	13.02.15 Morgen	13.02.14 Nachmittag	16.02.15 Morgen	16.02.15 Nachmittag	17.02.15 Morgen	17.02.15 Nachmittag	18.02.15 Nachmittag	20.02.15 Morgen	20.02.15 Nachmittag	23.02.15 Morgen	23.02.15 Nachmittag	24.02.15 Morgen	24.02.15 Nachmittag	25.02.15 Nachmittag	27.02.15 Morgen
<b>Teil 1: Umfeld und Ablauf</b>																							
Zeitplan erstellen	Soll	4																					
	Ist		2																				
Aufgabenstellung erfassen	Soll	2																					
	Ist		0.5																				
Vorkenntnisse erfassen	Soll	0.5																					
	Ist		0.5																				
Vorarbeiten erfassen	Soll	0.5																					
	Ist		0.5																				
Firmenstandards erfassen	Soll	0.5																					
	Ist		1																				
Sitzung mit Ivan Cosic	Soll	1																					
	Ist		0.5																				
Abschlussbericht erfassen	Soll	4																					
	Ist		4																				
<b>Teil 2: Projektdokumentation</b>																							
<b>Initialisierung</b>																							
Ist / Soll analysieren	Soll	2																					
	Ist		1.75																				
Vorgehensziele / Systemziele definieren	Soll	2																					
	Ist		2.25																				
Anforderungen definieren	Soll	2.5																					
	Ist		2.5																				
Expertenbesuch 1	Soll	1																					
	Ist		1.5																				
Risikoanalyse erfassen	Soll	2																					
	Ist		2.5																				
Besprechung der Phase mit Ivan Cosic (Freigabe Phase)	Soll	1																					
	Ist		0.5																				
<b>Konzept</b>																							
Logserver Konzept erstellen	Soll	3.5																					
	Ist		5																				
Namenskonzept erstellen	Soll	0																					
	Ist		1.5																				
Monitoring-Konzept erstellen	Soll	2.5																					
	Ist		2.5																				
Berechtigungskonzept erstellen	Soll	1																					
	Ist		1																				
Testkonzept erstellen	Soll	2																					
	Ist		3																				
Backupkonzept erstellen	Soll	1																					
	Ist		1.5																				
ISDS Konzept erstellen	Soll	1																					
	Ist		1																				
Besprechung der Phase mit Ivan Cosic (Freigabe Phase)	Soll	1																					
	Ist		1																				

Tabelle 6: Zeitplan - Teil 1

Tätigkeiten		Sollzeit in Stunden	Istzeit in Stunden	09.02.15 Morgen	09.02.15 Nachmittag	10.02.15 Morgen	10.02.15 Nachmittag	11.02.15 Nachmittag	13.02.15 Morgen	13.02.14 Nachmittag	16.02.15 Morgen	16.02.15 Nachmittag	17.02.15 Morgen	17.02.15 Nachmittag	18.02.15 Nachmittag	20.02.15 Morgen	20.02.15 Nachmittag	23.02.15 Morgen	23.02.15 Nachmittag	24.02.15 Morgen	24.02.15 Nachmittag	25.02.15 Nachmittag	27.02.15 Morgen
<b>Realisierung</b>																							
Grundinstallation Logserver	Soll	2																					
	Ist		2																				
Installation / Konfiguration Graylog Server	Soll	3																					
	Ist		3.5																				
Installation / Konfiguration Graylog Web	Soll	1																					
	Ist		0.5																				
Installation / Konfiguration Logstash	Soll	2																					
	Ist		4																				
Installation / Konfiguration Backup	Soll	1.5																					
	Ist		1																				
Installation / Konfiguration nginx	Soll	1.5																					
	Ist		1																				
Installation / Konfiguration der sendenden Hosts	Soll	7																					
	Ist		6																				
Konfiguration Monitoring	Soll	4																					
	Ist		4																				
Testen des Systems	Soll	3																					
	Ist		3																				
Systemdokumentaion erstellen	Soll	2																					
	Ist		2																				
Besprechung der Phase mit Ivan Cosic (Freigabe Phase)	Soll	1																					
	Ist		1																				
<b>Abschluss</b>																							
Management Summary	Soll	2																					
	Ist		2																				
Glossar / Quellenverzeichnis	Soll	2																					
	Ist		2																				
Expertenbesuch 2	Soll	1																					
	Ist		1																				
Korrekturen, Druck & binden	Soll	6																					
	Ist		6																				
<b>Fortlaufende Tätigkeiten</b>																							
Arbeitsjournal	Soll	6																					
	Ist		6																				
<b>Total</b>		80	81.5																				
SOLL												IST											
Meilenstein																							

Tabelle 7: Zeitplan - Teil 2



## 12.1 Meilensteine

Nr.	Name	Beschreibung
1	Teil 1 abgeschlossen	Teil 1: Umfeld und Ablauf ist abgeschlossen.
2	Phase „Initialisierung“ abgeschlossen	Die Phase „Initialisierung“ der IPA ist abgeschlossen.
3	Phase „Konzept“ abgeschlossen	Die Phase „Konzept“ der IPA ist abgeschlossen
4	Phase „Realisierung“ abgeschlossen	Die Phase „Realisierung“ der IPA ist abgeschlossen
5	IPA abgeschlossen	Die IPA Arbeit ist abgeschlossen, gedruckt, verschickt und hochgeladen. In einigen Tagen folgt die Präsentation und Demonstration der Arbeit.

Tabelle 8: Zeitplan

## 13. Arbeitsjournal

Die Festlegungen dieses Dokuments gelten im Projekt.  
Gemäss Art. 5 Absatz 2 der Wegleitung über die individuelle praktische Arbeit (IPA) an  
Lehrabschlussprüfungen des BBT vom 27. August 2001 gilt:

*„Die zu prüfende Person führt ein Arbeitsjournal. Sie dokumentiert darin täglich das Vorgehen, den Stand der Prüfungsarbeit, sämtliche fremde Hilfestellungen und besondere Vorkommnisse wie z.B. Änderungen der Aufgabenstellung, Arbeitsunterbrüche, organisatorische Probleme, Abweichungen von der Soll-Planung.“*

Das Arbeitsjournal zur IPA ist zwingend zu führen und den Experten und Fachvorgesetzten vorzulegen. Das Arbeitsjournal ist täglich sinngemäss und korrekt auszufüllen.

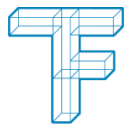
Das Arbeitsjournal dient der Nachvollziehbarkeit der von den Lernenden ausgeführten Arbeiten und wird als Teil der IPA in die Bewertung miteinbezogen.

### 13.1 Erster Tag: Montag, 09. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Zeitplan erstellen</b> Als ersten Schritt der IPA habe ich den Zeitplan erstellt. Da ich die Vorlage bereits im Vorfeld vorbereitet hatte, konnte ich den Zeitplan innert kurzer Zeit erstellen. Den Zeitplan habe ich im Microsoft Excel erstellt, damit ich ihn später in das Microsoft Word importieren kann.	F. Imobersteg	4	2
<b>Aufgabenstellung erfassen</b> Ich habe die Aufgabenstellung weitestgehend von PkOrg übernommen. Aus diesem Grund war die Aufgabenstellung schnell erfasst.	F. Imobersteg	2	0.5
<b>Vorkenntnisse erfassen</b> Die Liste der Vorkenntnisse stammt ebenfalls von PkOrg. Ich habe sie jedoch mit Beschreibungen mit meinen eigenen Worten ergänzt.	F. Imobersteg	0.5	0.5
<b>Vorarbeiten erfassen</b> Die Vorarbeiten stammen zum Teil von PkOrg. Ich habe jedoch jeden Punkt noch mit meinen eigenen Worten ergänzt.	F. Imobersteg	0.5	0.5
<b>Firmenstandards erfassen</b> Ich habe die Firmenstandards der TF Bern erfasst, welche diese IPA betreffen. Einige wichtige Dokumente dazu habe ich in den Anhang gepackt.	F. Imobersteg	0.5	1



<b>Sitzung mit Ivan Cosic</b> Zusammen mit Ivan Cosic konnte ich den Teil 1 der IPA besprechen. Er war mit dem Teil 1 zufrieden und hatte keine Anpassungen.	F. Imobersteg I. Cosic	0.5	0.5
<b>Ist / Soll analysieren</b> Ich habe den Ist- und Sollzustand festgehalten. Mithilfe der genauen Ziele von PkOrg und meinem Selbststudium vor der IPA war dies schnell erledigt.	F. Imobersteg	0	1
<b>Vorgehensziele / Systemziele definieren</b> Als nächsten Schritt habe ich die Vorgehens- und Systemziele erfasst. Ich habe mich grob an den Beurteilungskriterien und Anforderungen aus PkOrg orientiert.	F. Imobersteg	0	1.5
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben. Wie immer dauerte dies rund 30 Minuten.	F. Imobersteg	0	0.5
<b>Total:</b>		<b>8</b>	<b>8</b>
<b>Probleme und Erfolge</b>			
Als ich heute am Morgen in die Technische Fachschule Bern kam, war ich topmotiviert, mit der IPA endlich beginnen zu können. Grundsätzlich ist mir die Arbeit von heute sehr gut von der Hand gegangen. Einzig mit dem Erfassen der Firmenstandards hatte ich einige Probleme, da wir vor einiger Zeit eine Migration hatten und viele Dokumente noch nicht für das neue, heutige System angepasst sind. Zusammen mit Ivan Cosic konnte ich jedoch die notwendigen herausuchen. Einzig das Namenskonzept muss ich selber erfassen, da dies überhaupt nicht mehr mit der aktuellen Situation übereinstimmt.			
<b>Hilfestellungen</b>			
Ivan Cosic hat mir einige Fragen zu den Firmenstandards beantwortet.			
<b>Reflexion</b>			
Der Zeitplan war schneller erstellt als erwartet. Dies hängt sicher damit zusammen, dass ich bereits im Vorfeld der IPA eine Vorlage erstellt habe, welche ich jetzt nur noch ausfüllen musste. In Zukunft würde ich das wieder so machen, da ich auf diese Weise viel Zeit sparen konnte. Auch die Dokumentenvorlage war bereits vorbereitet, so dass ich direkt mit der eigentlichen Arbeit beginnen konnte. Das Erfassen der Vorarbeiten und Vorkenntnisse war schnell erfasst, da ich die Punkte von PkOrg übernehmen konnte und lediglich mit meinen eigenen Worten ergänzen musste. Als ich die Firmenstandards erfassen musste, stand ich vor dem Problem, dass viele unserer Dokumente über Firmenstandards nicht mehr auf dem aktuellen Stand sind. Wir hatten vor einiger Zeit eine Migration von Novell Server auf Windows Server und Windows XP Clients auf Windows 7. Die Anpassung vieler Dokumente ist dabei wohl einfach untergegangen. Zusammen mit Ivan Cosic konnte ich den Teil 1 der IPA besprechen. Ich war froh, dass er keine Änderungen mehr hatte und ich mit der Initialisierung beginnen konnte. Das Festhalten des Ist- und Sollzustandes stellte mich vor keine grossen Probleme, da ich mich am Beschrieb unter PkOrg orientieren konnte.			



Bei den Vorgehens- und Systemzielen musste ich etwas mehr überlegen. Ich war jedoch letztendlich auch schneller fertig als erwartet.

Ich habe jetzt einen Vorsprung gegenüber dem Zeitplan. Ein Vorsprung ist jedoch immer besser, als im Rückstand zu sein. Ich denke, dass ich die gewonnene Zeit schon noch irgendwo benötigen werde. Schliesslich sind bis jetzt noch kaum Probleme aufgetreten. Und früher oder später geschieht dies wohl in jedem Projekt

#### Nächste Schritte

- Ist und Soll überarbeiten
- Vorgehens- und Systemziele überarbeiten
- Ersten Expertenbesuch vorbereiten
- Expertenbesuch durchführen
- Anforderungen definieren
- Risikoanalyse erfassen

Tabelle 9: Arbeitsjournal: Montag, 09. Februar 2015

### 13.2 Zweiter Tag: Dienstag, 10. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Ist / Soll analysieren</b> Als ersten Schritt habe ich die Ist und Soll Analyse von gestern ergänzt und überarbeitet.	F. Imobersteg	1	0.75
<b>Vorgehensziele / Systemziele definieren</b> Als zweiten Schritt habe ich die Vorgehens- und Systemziele von gestern ergänzt und überarbeitet.	F. Imobersteg	1	0.75
<b>Anforderungen definieren</b> Als nächsten Schritt habe ich die funktionalen und nicht funktionalen Anforderungen definiert.	F. Imobersteg	2.5	2.5
<b>Expertenbesuch 1</b> Kurz vor dem Mittag habe ich die bereits bestehende Arbeit für den Expertenbesuch ausgedruckt und mich darauf vorbereitet. Am Nachmittag hat der Besuch stattgefunden.	F. Imobersteg	1	1.5
<b>Risikoanalyse erfassen</b> Ich habe die Risikoanalyse und die Risikographen erstellt.	F. Imobersteg	2	2
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>8</b>	<b>8</b>



### Probleme und Erfolge

Der Expertenbesuch ist sehr gut verlaufen. Leider war der Co-Experte, Herr Imboden, verhindert und konnte nicht teilnehmen. Ich denke, dass das Kennenlernen gut verlaufen ist. Ich konnte einige wichtige Erkenntnisse aus dem Besuch mitnehmen.

Eine Erkenntnis daraus war, dass die Tabellen in meinem Dokument nicht bündig mit dem Text waren. Ich habe einige Zeit gesucht und letztendlich herausgefunden, dass dies Standard im Word 2010 ist. Schliesslich habe ich mir eine Tabellenvorlage erstellt. Schade, wie viel Zeit mit der Neuformatierung des Dokuments verloren gegangen ist.

Ebenfalls beim Expertenbesuch habe ich erfahren, dass die Form des gestrigen Arbeitsjournals noch verbesserungswürdig ist. Herr Tschannen wird mir noch eine Vorlage als Beispiel zukommen lassen. Ich werde, sobald ich die Vorlage erhalten habe, das Journal in der angepassten Form weiterführen.

### Hilfestellungen

Heute war ich auf keine Hilfe von aussen angewiesen.

### Reflexion

Die eigentliche Arbeit und der Expertenbesuch sind sehr gut verlaufen. Ich habe jedoch viel zu viel Zeit mit der Word Formatierung verloren. Ich werde in zukünftigen Projekten ähnlicher Tragweite in Erwägung ziehen, das Dokument in Latex zu schreiben. Unter Umständen könnte ich mich da mehr um den Inhalt und weniger um die Formatierung kümmern.

### Nächste Schritte

- Initialisierungsphase abschliessen
- Sitzung mit Ivan Cosic
- Beginn mit Logserver Konzept

Tabelle 10: Arbeitsjournal: Dienstag, 10. Februar 2015

## 13.3 Dritter Tag: Mittwoch, 11. Februar 2015 (halber Tag)

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Besprechung der Initialisierungsphase</b> Als ich heute ankam, habe ich gemeinsam mit Ivan Cosic die Initialisierungsphase besprochen und die Phase für abgeschlossen erklärt.	F. Imobersteg I. Cosic	1	0.5
<b>Logserver Konzept erstellen</b> Als nächsten Schritt habe ich mit dem Logserver Konzept begonnen. Ich bin nicht ganz so weit gekommen, wie ich erwartet hatte.	F. Imobersteg	2.5	3
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5



<b>Total:</b>		<b>4</b>	<b>4.5</b>
<b>Probleme und Erfolge</b>			
<p>Heute habe ich die Initialisierungsphase abgeschlossen. Was für ein tolles Gefühl, den ersten Meilenstein zu erreichen!</p> <p>Mit dem Logserverkonzept bin ich etwas weniger weit gekommen, als ich erwartete. Da ich aber nach wie vor einen Vorsprung gegenüber dem Zeitplan habe, ist dies nicht weiter ein Problem. Weiter habe ich heute festgestellt, dass das bestehende Namenskonzept der TF Bern überhaupt nicht mehr der Realität entspricht. Ich bin mit Ivan Cosic so verblieben, dass ich den relevanten Teil davon im Rahmen der IPA erarbeite.</p>			
<b>Hilfestellungen</b>			
<p>Heute war ich auf keine fremden Hilfestellungen angewiesen.</p>			
<b>Reflexion</b>			
<p>Leider hatte ich das Namenskonzept, welches nicht mehr gültig ist, nicht auf dem Schirm. Ich werde aus diesem Grund etwas Zeit verlieren. Ich hatte den Firmenstandards im Vorfeld der IPA wohl zu wenig Beachtung geschenkt.</p> <p>Zum Glück habe ich einen gewissen Vorsprung auf den Zeitplan, sodass dies nicht wirklich ein Problem ist, wenn ich dies jetzt noch erstellen muss.</p>			
<b>Nächste Schritte</b>			
<ul style="list-style-type: none"><li>• Logserverkonzept fertigstellen</li><li>• Namenskonzept erstellen</li><li>• Monitoring-Konzept erstellen</li></ul>			

Tabelle 11: Arbeitsjournal: Mittwoch, 11. Februar 2015 (halber Tag)

### 13.4 Vierter Tag: Freitag, 13. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Logserver Konzept erstellen</b> Als ersten Schritt habe ich das gestern begonnene Logserver Konzept abgeschlossen.	F. Imobersteg	2	2
<b>Namenskonzept erstellen</b> Als nächsten Schritt habe ich das Namenskonzept erstellt, da kein aktuelles mehr vorhanden war.	F. Imobersteg	1.5	1.5
<b>Monitoring-Konzept erstellen</b> Nach dem Mittag habe das Monitoring-Konzept begonnen.	F. Imobersteg	2.5	2.5
<b>Berechtigungskonzept erstellen</b> Zum Schluss habe ich das Berechtigungskonzept erstellt.	F. Imobersteg	1	1



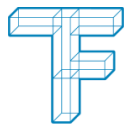


<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>7.5</b>	<b>7.5</b>
<b>Probleme und Erfolge</b>			
Das Erstellen des Logserverkonzepts hat insgesamt etwas länger als geplant gedauert. Ich denke aber, dass sich die mehrgenutzte Zeit ausbezahlt hat. Mit dem Konzeptionieren des Monitorings hatte ich etwas Mühe. Mir war zu Beginn nicht klar, was in ein Monitoring-Konzept gehört. Das Erfassen des Berechtigungskonzepts hat mir keine grosse Mühe bereitet.			
<b>Hilfestellungen</b>			
Heute war ich auf keine fremden Hilfestellungen angewiesen.			
<b>Reflexion</b>			
Heute bin ich im Grossen und Ganzen gut vorangekommen. Leider habe ich mich beim Erstellen des Zeitplans etwas mit der Dauer überschätzt, welche ich zum Erfassen des Logserverkonzepts benötige. Da sich aber der Aufwand gelohnt hat und ich dem Zeitplan voraus bin, sehe ich meine Fehler als nicht allzu grosses Problem.			
<b>Nächste Schritte</b>			
<ul style="list-style-type: none"><li>• Testkonzept erstellen</li><li>• Backupkonzept erstellen</li><li>• ISDS Konzept erstellen</li><li>• Besprechung und Abschluss der Phase Konzept mit Ivan Cosic</li></ul>			

Tabelle 12: Arbeitsjournal: Freitag, 13. Februar 2015

### 13.5 Fünfter Tag: Montag, 16. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Testkonzept erstellen</b> Als ersten Schritt habe ich das Testkonzept erstellt.	F. Imobersteg	2	3
<b>Backupkonzept erstellen</b> Als nächsten Schritt habe ich das Backupkonzept geschrieben.	F. Imobersteg	1	1.5
<b>ISDS Konzept erstellen</b> Nach dem Mittag habe ich das ISDS Konzept festgehalten.	F. Imobersteg	1	1



<b>Besprechung der Phase mit Ivan Cosic</b> Zum Abschluss der Phase „Konzept“ habe ich diese mit Ivan Cosic besprochen	F. Imobersteg I. Cosic	1	1
<b>Grundinstallation Logserver</b> Nun konnte ich endlich mit der Realisation beginnen und den Logserver installieren. Diese Arbeit werde ich morgen fertigstellen.	F. Imobersteg	2	1
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>7.5</b>	<b>8</b>
<b>Probleme und Erfolge</b>			
<p>Heute habe ich die zweite Phase, das Konzept abgeschlossen. Nun konnte ich endlich mit der Realisierung beginnen. Ich habe mich richtiggehend darauf gefreut.</p> <p>Bei den meisten Punkten von heute hatte ich etwas länger als geplant. Dies hängt aber sicherlich auch damit zusammen, dass ich noch die Themen von den Vortagen überarbeitet habe. Ich bin nach wie vor gut im Zeitplan.</p> <p>Zusammen mit Ivan Cosic habe ich festgestellt, dass aus der Aufgabenstellung nicht klar herausgeht, ob die Systemdokumentation ein separates Dokument sein soll und was genau darin beschrieben werden soll. Wir haben uns darauf geeinigt, dass die in der detaillierten Aufgabenstellung festgelegten Inhalte der Systemdokumentation im Konzept- bzw. der Realisierungsdokumentation festgehalten werden. Ein separates Dokument ist nicht notwendig, da dadurch nur unnötige Redundanzen entstehen würden.</p>			
<b>Hilfestellungen</b>			
Heute war ich auf keine Hilfestellungen angewiesen.			
<b>Reflexion</b>			
<p>Heute bin ich im Grossen und Ganzen gut vorangekommen. Über das Wochenende habe ich mir die Zeit genommen, den Text durchzulesen und Unklarheiten sowie Fehler zu markieren. Auf diese Weise konnte ich heute die bisherigen Teile speditiv überarbeiten. Ich werde dies am nächsten Wochenende wiederholen, da sich dies bewährt hat.</p> <p>Mit dem Testkonzept habe ich etwas mehr Zeit benötigt als erwartet. Dies hängt sicherlich damit zusammen, dass diese IPA viele Einzelkomponenten besitzt, welche einzelne Testfälle benötigen. In einem zukünftigen, ähnlichen Projekt würde ich etwas mehr Zeit für das Testkonzept reservieren.</p>			
<b>Nächste Schritte</b>			
<ul style="list-style-type: none"><li>• Grundinstallation Logserver</li><li>• Installation Konfiguration / Konfiguration Graylog Web</li><li>• Installation Logstash</li><li>• Führen der Systemdokumentation</li></ul>			

Tabelle 13: Arbeitsjournal: Montag, 16. Februar 2015



### 13.6 Sechster Tag: Dienstag, 17. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Grundinstallation Logserver</b> Als ich heute angekommen bin, habe ich die begonnene Arbeit von gestern, nämlich die Grundinstallation des Logservers, abgeschlossen.	F. Imobersteg	1	1
<b>Installation / Konfiguration Graylog Server</b> In einem nächsten Schritt habe ich den Graylog Server Dienst inklusive allen Abhängigkeiten in Betrieb genommen.	F. Imobersteg	3	3.5
<b>Installation / Konfiguration Graylog Web</b> Anschliessend habe ich den Graylog Web Dienst installiert und alle notwendigen Konfigurationen vorgenommen.	F. Imobersteg	1	0.5
<b>Installation / Konfiguration Logstash</b> Später habe ich Logstash Konfiguration begonnen. Als ich das Ganze testen wollte, stellte ich fest, dass keine paketierte Logstash-Forwarder Version mehr für Debian verfügbar ist. Leider ist die Konfiguration noch nicht ganz abgeschlossen.	F. Imobersteg	2	3
<b>Systemdokumentaion erstellen</b> Fortlaufend habe ich die aufgetretenen Probleme analysiert und deren Lösung dokumentiert.	F. Imobersteg	0.5	0.5
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>8</b>	<b>9</b>
<b>Probleme und Erfolge</b>			
<p>Mit der Installation der Graylog Servers habe ich etwas länger gebraucht als erwartet. Es mussten sehr viele Abhängigkeiten installiert werden und dies hat einfach seine Zeit gedauert. Dafür war ich mit der Graylog Web Installation etwas schneller.</p> <p>Grosse Probleme hatte ich bei der Installation von Logstash. Als ich die ersten Konfigurationen vorgenommen hatte, und das Ganze testen wollte, habe ich festgestellt, dass vor wenigen Tagen das Logstash-Forwarder aus dem offiziellen Repository entfernt wurde. Aus diesem Grund musste ich das Paket selbst erstellen. Da ich dies vorher noch nie gemacht habe und viele Abhängigkeiten bestanden, welche aufgrund veralteter Pakete manuell gelöst werden mussten, hat dies lange gedauert.</p>			
<b>Hilfestellungen</b>			
Heute war ich auf keine Hilfestellungen angewiesen.			

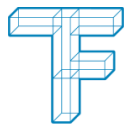


Reflexion
Heute bin ich, abgesehen von dem nicht mehr verfügbaren Logstash-Forwarder Paket, gut vorangekommen. Ich denke nicht, dass sich dieses Problem hätte vorhersehen lassen. Aus diesem Grund hätten auch keine sinnvollen Vorkehrungen getroffen werden können. Ich habe zwar einige Zeit verloren, aber auch viel beim Erstellen des Pakets gelernt.
Nächste Schritte
<ul style="list-style-type: none"><li>• Konfiguration Logstash abschliessen</li><li>• Installation / Konfiguration Backup vornehmen</li><li>• nginx Installation / Konfiguration beginnen</li></ul>

Tabelle 14: Arbeitsjournal: Dienstag, 17. Februar 2015

### 13.7 Siebter Tag: Mittwoch, 18. Februar 2015 (halber Tag)

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Installation / Konfiguration Logstash</b> In einem ersten Schritt habe ich die gestern begonnene Logstash Konfiguration abgeschlossen.	F. Imobersteg	0	1
<b>Installation / Konfiguration Backup</b> Anschliessend habe ich das Backupscript erstellt und alle benötigten Softwarepakete installiert.	F. Imobersteg	1.5	1
<b>nginx Installation / Konfiguration</b> Als nächstes habe ich nginx installiert und konfiguriert.	F. Imobersteg	1.5	1
<b>Systemdokumentaion erstellen</b> Ich habe ich die Verwendung des Backupscripts dokumentiert	F. Imobersteg	0.5	0.5
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>4</b>	<b>4</b>
Probleme und Erfolge			
Der heutige Arbeitstag verlief weitestgehend ohne Probleme. Dies hat sicher damit zu tun, dass ich die heutigen Schritte bereits mehrfach zu einem früheren Zeitpunkt durchgeführt habe.			
Hilfestellungen			
Heute war ich auf keine Hilfestellungen angewiesen.			

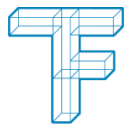


Reflexion
Wenn die Arbeit so gut wie heute weiterläuft, bin ich voll und ganz zufrieden. Es ist fast schon langweilig, so gut wie keine Probleme zu haben.
Nächste Schritte
<ul style="list-style-type: none"><li>• Installation der sendenden Hosts</li><li>• Weiterarbeit an der Systemdokumentation</li></ul>

Tabelle 15: Arbeitsjournal: Mittwoch, 18. Februar 2015 (halber Tag)

### 13.8 Achter Tag: Freitag, 20. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Installation / Konfiguration der sendenden Hosts</b> Zu Beginn habe ich heute die Scripts für die automatische Installation der sendenden Server erstellt. Anschliessend habe ich die sendenden Hosts installiert und konfiguriert.	F. Imobersteg	7	6
<b>Konfiguration Monitoring</b> Anschliessend habe ich mit der Konfiguration des Monitorings begonnen.	F. Imobersteg	0	1
<b>Systemdokumentaion erstellen</b> Fortlaufend habe ich die aufgetretenen Probleme analysiert und deren Lösung dokumentiert.	F. Imobersteg	0.5	0.5
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>8</b>	<b>8</b>
Probleme und Erfolge			
Das Erstellen der Scripts und die anschliessende Konfiguration der sendenden Server hat sehr gut und speditiv funktioniert. Mit diesem Teil war ich schneller fertig als erwartet. Auch die Switches waren rascher als erwartet konfiguriert. Leider hatte ich danach mit der Konfiguration der Router erhebliche Probleme. Es liess sich nicht wie erwartet das Source Interface des Logversands setzen, sondern es hätten weit grössere Änderungen vorgenommen werden müssen, welche den laufenden Schulbetrieb erheblich gefährdet hätten. Nach Absprache mit dem Fachvorgesetzten Ivan Cosic kamen wir zum Schluss, dass die Konfigurationsänderungen der beiden Router nicht im Rahmen dieser IPA vorgenommen werden. Der gewonnene Mehrwert hätte in keinem Verhältnis zu dem Risiko eines Unterbruchs und dem Aufwand gestanden.			



Hilfestellungen
Für die Entscheidung, wie mit dem Problem der erschwerten Router Konfiguration vorgegangen werden soll, war ich auf die Hilfe von Ivan Cosic angewiesen.
Reflexion
Abgesehen von der Router Konfiguration bin ich heute sehr gut vorwärts gekommen. Besonders die Installationsscripts haben sich bestens bewährt. Auch das Testing der Scripts in einer Vagrant VM war die richtige Entscheidung. Einzig die nicht mögliche Konfiguration der Router ärgert mich.
Nächste Schritte
<ul style="list-style-type: none"><li>• Abschluss der Monitoring-Konfiguration</li><li>• Testen des Systems</li><li>• Abschliessen der Systemdokumentation</li><li>• Abschliessen der Realisierung</li></ul>

Tabelle 16: Arbeitsjournal: Freitag, 20. Februar 2015

### 13.9 Neunter Tag: Montag, 23. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Konfiguration Monitoring</b> Als ersten Schritt habe ich die Konfiguration des Monitorings abgeschlossen.	F. Imobersteg	3	3
<b>Testen des Systems</b> Anschliessend habe ich gemeinsam mit Hetem Shaqiri das System getestet.	F. Imobersteg H. Shaqiri	3	3
<b>Systemdokumentaion erstellen</b> Ich habe die Systemdokumentation ergänzt und abgeschlossen.	F. Imobersteg	0.5	0.5
<b>Besprechung der Phase mit Ivan Cosic</b> Gemeinsam mit Ivan Cosic habe ich die Phase „Realisierung“ besprochen und abgeschlossen.	F. Imobersteg I. Cosic	1	1
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>8</b>	<b>8</b>
Probleme und Erfolge			
Heute bin ich gut vorangekommen. Ich konnte die Phase der Realisierung abschliessen. Auch diese Phase habe ich gemäss dem Zeitplan abgeschlossen. Nun bin ich schon im Schlusspurt der IPA. Einzig mit dem Check ob der Prozess „logstash-forwarder“ auf den Linux Server läuft, hatte ich			



etwas Mühe. Da ich kein passendes Icinga bzw. Nagios Plugin gefunden habe, musste ich ein eigenes erstellen.

#### Hilfestellungen

Heute war ich auf keine Hilfestellungen angewiesen.

#### Reflexion

Heute bin ich ziemlich genau nach dem Zeitplan vorangekommen. Ich hoffe, dass es so weiter geht. Es freut mich, dass ich nach wie vor im Zeitplan liege.

#### Nächste Schritte

- Management Summary schreiben
- Glossar und Quellenverzeichnis erstellen
- Expertenbesuch 2
- Abschlussbericht erstellen

Tabelle 17: Arbeitsjournal: Montag, 23. Februar 2015

### 13.10 Zehnter Tag: Dienstag, 24. Februar 2015

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Management Summary</b> In einem ersten Schritt habe ich das Management Summary geschrieben.	F. Imobersteg	2	2
<b>Glossar / Quellenverzeichnis</b> Anschliessend habe ich das Glossar und Quellenverzeichnis erstellt.	F. Imobersteg	2	2
<b>Expertenbesuch 2</b> Am Nachmittag hat der zweite Expertenbesuch stattgefunden.	F. Imobersteg	1	1
<b>Abschlussbericht erfassen</b> Nach dem Expertenbesuch habe ich den Abschlussbericht begonnen.	F. Imobersteg	2.5	2.5
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>8</b>	<b>8</b>



Probleme und Erfolge
Das einzige Problem das ich heute hatte war, dass mir nicht klar war, wie ein Management Summary genau aussehen muss. Mithilfe des Internets konnte ich dies aber schnell herausfinden. Der restliche Teil lief wie geplant und sehr gut.
Hilfestellungen
Heute war ich auf keine Hilfestellungen angewiesen.
Reflexion
Der heutige Tag verlief sehr gut. Auch der Expertenbesuch verlief nach Plan. Nun geht's nur noch an das Fertigstellen des Abschlussberichts, das Korrigieren und Überarbeiten.
Nächste Schritte
<ul style="list-style-type: none"><li>• Abschlussbericht erfassen</li><li>• Korrekturen, Druck &amp; binden</li></ul>

Tabelle 18: Arbeitsjournal: Dienstag, 24. Februar 2015

### 13.11 Elfter Tag: Mittwoch, 25. Februar 2015 (halber Tag)

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Abschlussbericht erfassen</b> Am Morgen habe ich den Abschlussbericht fertiggestellt.	F. Imobersteg	1.5	1.5
<b>Korrekturen, Druck &amp; binden</b> Anschliessend habe ich mit der Korrektur begonnen.	F. Imobersteg	2	2
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>4</b>	<b>4</b>
Probleme und Erfolge			
Heute habe ich alle Texte der Dokumentation fertiggestellt. Jetzt muss ich lediglich noch die Korrektur abschliessen und die Texte überarbeiten. Es ist fast schon schade, dass der Umsetzungsteil der IPA schon vorbei ist.			
Hilfestellungen			
Heute war ich auf keine Hilfestellungen angewiesen.			



<b>Reflexion</b>
Heute bin ich gut vorangekommen. Ich muss lediglich noch die Korrekturen abschliessen und die Arbeit versenden. Ein tolles Gefühl.
<b>Nächste Schritte</b>
<ul style="list-style-type: none"> <li>Korrekturen, Druck &amp; binden</li> </ul>

Tabelle 19: Arbeitsjournal: Mittwoch, 25. Februar 2015 (halber Tag)

### 13.12 Zwölfter Tag: Freitag, 27. Februar 2015 (halber Tag)

Tätigkeiten	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
<b>Korrekturen, Druck &amp; binden</b> Heute habe ich die Korrekturen abgeschlossen, das Dokument gebunden und verschickt.	F. Imobersteg	4	4
<b>Arbeitsjournal</b> Wie an jedem Tag der IPA, habe ich das tägliche Arbeitsjournal geschrieben.	F. Imobersteg	0.5	0.5
<b>Total:</b>		<b>4.5</b>	<b>4.5</b>
<b>Probleme und Erfolge</b>			
<p>Heute hatte ich nur kleinere Probleme. Diese hatten hauptsächlich mit den Formatierungseinstellungen des Words zu tun.</p> <p>Der Umsetzungsteil der IPA ist mit diesem Tag abgeschlossen. Ein tolles Gefühl! Nun folgt nur noch die Präsentation, Demonstration und das Fachgespräch.</p>			
<b>Hilfestellungen</b>			
Heute war ich auf keine Hilfestellungen angewiesen.			
<b>Reflexion</b>			
Den Abschlusstag in einer weiteren ähnlichen Arbeit, würde ich genauso wie den heutigen handhaben.			
<b>Nächste Schritte</b>			
<ul style="list-style-type: none"> <li>Präsentation</li> <li>Demonstration</li> <li>Fachgespräch</li> </ul>			

Tabelle 20: Arbeitsjournal: Freitag, 27. Februar 2015 (halber Tag)



### 13.13 Arbeitszeit total

Totaler Zeitaufwand	Person	Aufwand geplant (Std)	Aufwand effektiv (Std)
	F. Imobersteg	80	81.5

Tabelle 21: Arbeitszeit total



## 14. Abschlussbericht

Der Umsetzungsteil der individuellen praktischen Arbeit ist nun vollendet. Wenn ich auf die zurückliegenden 12 Arbeitstage zurückblicke, kann ich mit Stolz sagen, dass ich das Projekt erfolgreich abgeschlossen habe.

In rund einer Woche werden die Präsentation mit anschliessender Demonstration, das Fachgespräch und die Auswertung stattfinden.

### 14.1 Vergleich Ist/Soll

Die Umsetzung des Projektes wurde wie geplant durchgeführt. Im Vorfeld wurde ein Konzept erstellt, um die Vorgehensweise und Methoden zu definieren.

Sämtliche, durch meinen Fachvorgesetzten vorgegeben Ziele wurden erfüllt. Der Logserver konnte mit den zur Verfügung stehenden Mitteln installiert und konfiguriert werden. Die sendenden Hosts konnten mit Ausnahme der Router alle wie gewünscht konfiguriert werden. Bei den Routern war es leider nicht möglich, diese wie erwartet zu konfigurieren. Gemeinsam mit dem Fachvorgesetzten fiel die Entscheidung, diesen Teil nicht während der IPA umzusetzen, da die notwendigen Konfigurationsanpassungen den laufenden Schulbetrieb erheblich gefährdet hätten und der dabei entstandene Mehrwert in keinem Verhältnis zu dem Risiko eines Ausfalls gestanden hätte. Ebenfalls gemeinsam mit dem Fachvorgesetzten Ivan Cosic wurde entschieden, dass die Systemdokumentation kein separates Dokument, sondern die notwendigen Kapitel im Realisierungsbericht untergebracht werden. Auf diese Weise wurden unnötige Redundanzen vermieden.

### 14.2 Mittelbedarf

Es wurden die auf der Seite 17 aufgeführten Mittel verwendet. Es mussten keine weiteren Mittel beschafft oder verwendet werden.

### 14.3 Realisierungsbericht

Die Realisierung des Projekts konnte gemäss dem Zeitplan abgeschlossen werden. Mit Ausnahme der Konfiguration der sendenden Router konnte alles in der vorgegebenen Zeit realisiert werden. Unter Absprache mit dem Fachvorgesetzten Ivan Cosic wurde auf die Konfiguration der beiden Router verzichtet, da die notwendigen Anpassungen den laufenden Schulbetrieb gefährdet hätten. Weiter hatte ich das Problem, dass keine Logstash-Forwarder Paket im offiziellen Repository mehr verfügbar ist. Die frühere Version wurde vom Entwicklerteam gelöscht, da diese von einem Bug betroffen ist. Aus diesem Grund habe ich mich entschieden, aus der aktuellen Version selber ein Paket zu erstellen. Fortlaufend wurde die Dokumentation nachgeführt und überarbeitet.

### 14.4 Testbericht

Das Testing wurde von Hetem Shaqiri (Testperson) und Felix Imobersteg (Projektleiter) durchgeführt. Alle 15 Testfälle wurden gemäss dem Drehbuch durchgeführt. Ein Testergebnis des Testfalls 8 war nicht wie erwartet, da die beiden Router nicht konfiguriert wurden (siehe „Vergleich Ist/Soll“). Bei allen anderen Testfällen, ist das Ergebnis so wie erwartet eingetreten.



## 14.5 Fazit zum Projekt

Das Projekt wurde erfolgreich in der vorgegebenen Zeit abgeschlossen. Es wurden alle Anforderungen und Ziele erfüllt und getestet. Es wurde ein gut strukturierter Zeitplan erstellt, welcher meistens eingehalten werden konnte. Alle Meilensteine wurden zur vorgegebenen Zeit erreicht. Sämtliche Anforderungen, mit Ausnahme der Konfiguration der Router, wurden voll und ganz erfüllt. Das installierte Logmanagement kann ab sofort im produktiven Betrieb eingesetzt werden.

## 14.6 Persönliches Fazit

Meine IPA ist nun vollendet. Ein weiterer Meilenstein meiner Lehrzeit ist somit erreicht. Das Erstellen der Dokumentation bzw. das viele Schreiben war sehr erschöpfend. Zu Beginn der IPA war ich etwas nervös und wusste nicht recht, was auf mich zukommt. Dennoch habe ich mich sehr gefreut, die Arbeit durchzuführen.

Ich war erstaunt, wie genau die Zeitplanung hingehauen hat. Ich bin zwar hier und da Mal wieder eine halbe Stunde danebengelegen. Im Grossen und Ganzen hat es aber gepasst.

Während der Arbeit konnte ich mich zu einem grossen Teil auf mein Wissen verlassen. Falls ich Mal nicht weiter gewusst habe, habe ich meine Notizen vom Selbststudium angeschaut oder einfach gegoogelt. Bei fachlichen Fragen war ich während der Arbeit nie auf Hilfe von aussen angewiesen. Einzig wenn es darum ging, den Rahmen abzustecken, suchte ich ein Gespräch mit dem Fachvorgesetzten Ivan Cosic.

Ich war sehr erstaunt, welche Menge an Logs versendet wird. Zurzeit werden ca. 2 GB pro Tag versendet. Ich hatte zwar im Vorfeld der Arbeit Tests durchgeführt, wie viele Logs ungefähr zu erwarten sind, aber dabei nicht bedacht, wie viele Logeinträge auf dem Microsoft Exchange und dem Printserver entstehen. Da ich die Ressourcen mit genügend Reserve geplant habe, führt dies jetzt zu keinem Problem. Einzig der Festplattenspeicherplatz muss etwas im Auge behalten werden. Es werden immerhin rund 40 Lognachrichten pro Sekunde verarbeitet. Falls die Ressourcen in Zukunft einmal knapp werden sollten, lassen sich problemlos weitere Server hinzufügen und die Last aufteilen.

Wie aktiv und gewinnbringend das in diesem Projekt installierte System im Alltag des Ressorts Informatik eingesetzt wird, wird sich erst noch zeigen. Bisher hatte noch keiner der Mitarbeiter des Ressorts Informatik die Möglichkeit, auf ein derart ausgeklügeltes Logmanagementsystem zurückzugreifen. Sicherlich muss in Zukunft noch viel Knowhow im Team gewonnen werden. Erste Probleme wurden jedoch schon jetzt, durch Teammitglieder, mithilfe des in diesem Projekt installierten Systems erkannt.

Während den letzten Tagen habe ich auch viel Neues gelernt. Zum Beispiel habe ich vorher noch nie ein Debian Paket erstellt. Auch beim Erstellen des Nagios Plugins für die Überwachung des Logstash-Forwarder Prozesses habe ich etwas gelernt.

Ebenfalls habe ich bei der Verwendung der Projektmethode HERMES einiges gelernt. Ich werde mich aber auch in Zukunft nicht wirklich damit anfreunden können. Die agile und resultatsorientierte Arbeit mit Scrum liegt mir einfach mehr. Was nicht heissen soll, dass auch nicht HERMES seine Vorteile hat.

Ich bin stolz, dass ich diese Arbeit erfolgreich abgeschlossen und hoffe, dass ich zukünftige Arbeiten ebenso erfolgreich abschliessen kann.



## 15. Unterschriften Teil 1

Die lernende Person bestätigt mit ihrer Unterschrift diese IPA aus Eigenleistung erbracht und nach den Vorgaben der Prüfungskommission Informatik Kanton Bern erstellt zu haben. Die Angaben im Arbeitsjournal entsprechen dem geleisteten Arbeitsaufwand.


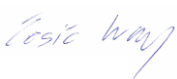
Datum	Name	Unterschrift
27.02.14	Felix Imobersteg Lernender	
27.02.14	Ivan Cosic Fachvorgesetzter	

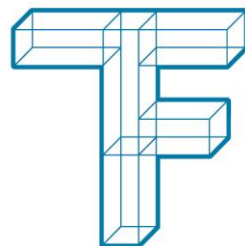
Tabelle 22: Unterschriften Teil 1



## Teil 2: Projektdokumentation

IPA Projektname:  
Autor:

Zentrales Logmanagement in Betrieb nehmen  
Felix Imobersteg



TECHNISCHE  
FACHSCHULE  
BERN

## 16. Projektmethode

Als Projektmethode wird Hermes 5 IPA verwendet. Hermes 5 IPA ist einer stark vereinfachte Form von Hermes 5.



Abbildung 4: Hermes 5 IPA

### 16.1 Erläuterung der Phasen

#### 16.1.1 Initialisierung

Die Initialisierung schafft eine definierte Ausgangslage für das Projekt und stellt sicher, dass die Projektziele mit PkOrg übereinstimmen. Die Projektgrundlagen und der Projektauftrag sind erarbeitet.

#### 16.1.2 Konzept

Die in der Phase „Initialisierung“ gewählte Variante wird konkretisiert, sowie weitere Konzepte erstellt. Die Ergebnisse werden so detailliert erarbeitet, dass eine aussenstehende Person (Experte) sämtliche Schritte nachvollziehen kann. Es muss klar ersichtlich sein, was, wie, wo und wann realisiert wird.

#### 16.1.3 Realisierung

Das Produkt bzw. das IT-System wird realisiert und getestet. Die nötigen Vorarbeiten werden geleistet, um die Einführungsrisiken zu minimieren. Braucht es noch ein „Re-Testing“ oder werden mögliche, kleine Fehler bei einem späteren Zeitpunkt noch korrigiert?

#### 16.1.4 Einführung

Der sichere Übergang vom alten zum neuen Zustand wird gewährleistet. Der Betrieb wird ggf. aufgenommen und so lange durch das Projekt unterstützt, bis er stabil ist. Die Dokumentationen werden pünktlich auf PkOrg hochgeladen. Das Projekt wird abgeschlossen und die „Projektorganisation“ wird aufgelöst. Danach folgen die Präsentation und die anschliessende Bewertung durch die Experten und Fachvorgesetzten. Eine eigentliche Einführungsphase ist nicht Teil der IPA Umsetzungsphase. Aus diesem Grund ist sie nicht in diesem Dokument ersichtlich.



## 17. Initialisierung

### 17.1 Studie Ist-Zustand / Soll-Zustand

#### 17.1.1 Istzustand

Zurzeit werden in der TF Bern keine Logs zentral gesammelt. Jeder Server, Switch oder Router speichert seine Logdateien lokal. Zur Suche in den Logs, können nur die Bordmittel auf dem jeweiligen Host verwendet werden. Dies wird vor allem dann problematisch, wenn nach einer spezifischen Information, wie zum Beispiel die IP-Adresse eines ungültigen SSH Logins, gesucht werden soll. Weiter ist es kaum möglich, einen Zeitverlauf oder Performance Daten darzustellen. Ein weiteres grosses Problem tritt auf, wenn Logs über mehrere Hosts durchsucht werden sollen. Nehmen wir einmal an, der Zugriff auf einen Server funktioniert nicht mehr. Die Fehlerursache kann von verschiedenen Geräten verursacht worden sein. Ein Netzwerkunterbruch ist genauso wahrscheinlich wie ein abgestürzter Webserverdienst. Besonders in einer solchen Situation ist es von Nöten, die Logs über mehrere Hosts durchsuchen zu können, was jedoch zurzeit nicht möglich ist.

#### 17.1.2 Sollzustand

In Zukunft sollen die Logs der TF Bern IT Infrastruktur zentral gesammelt werden. Zur Logverwaltung soll Graylog Server verwendet werden. Zur späteren Anzeige der Lognachrichten und Suche wird das Webinterface verwendet, welches ebenfalls von Graylog stammt. Zur grundlegenden Normalisierung der empfangenen Nachrichten wird Logstash installiert und konfiguriert. Alle Logverwaltungsdienste sollen gemeinsam auf einem einzelnen, zusätzlichen Debian Wheezy Server installiert werden. Es sollen, wo möglich und sinnvoll, Open Source Produkte verwendet werden.

Im Rahmen dieser IPA werden lediglich die Systemlogs der nachfolgenden Geräten an den Logserver gesendet:

- Windows Server (2008 R2 und 2012)
  - PHLIC1
  - PHBACKUP1
  - VMDB1
  - VMDC1
  - VMDC2
  - VMDC3
  - VMDC4
  - VMDC5
  - VMDIENST1
  - VMFSL1
  - VMFSS1
  - VMFSV1
  - VMIS1
  - VMMAIL1
  - VMORGA1
  - VMPRINT1





- Linux Server (Debian 7)
  - VMFILE1
  - VMMON1
  - VMRM1
  - VMWEB1
  - PHDR1
- Cisco Switches und Router
  - lo003-o01aa-sd1
  - lo003-o01aa-sa3
  - lo003-o01aa-sa4
  - lo003-o01ba-sa1
  - lo003-u01aa-sa1
  - lo003-u01aa-sa2
  - lo003-o01da-sa1
  - lo003-o01da-sa2
  - lo003-e00aa-sa1
  - lo003-o03aa-sa1
  - lo003-o02aa-sa1
  - lo003-o02aa-sa2
  - lo003-e00ba-sa1
  - lo003-e00ba-sa2
  - lo003-o01ca-sa1
  - lo003-o01ca-sa2
  - lo01b-u01aa-sa1
  - lo01b-u01ba-sa1
  - lo01b-u01ca-sa1
  - lo01b-u01da-sa1
  - lo01b-u02aa-sa1
  - fe017-u01aa-sd1
  - fe017-e00aa-sa1
  - fe017-u01aa-sa2
  - fe017-o01aa-sa1
  - fe017-e00ba-sa1
  - fe017-e00fa-sa1
  - fe017-o01ba-sa1
  - fe017-o01ba-sa2
  - fe017-o02aa-sa1
  - fe017-e00da-sa1
  - fe017-e00ea-sa1
  - fe017-e00ca-sa1

Dazu ist es notwendig, an jedem der Geräte den Versand einzurichten. Da unter Windows und Linux ein zusätzlicher Dienst installiert werden muss, wird dazu ein Script erstellt, welches die Installation vornimmt. Unter Cisco Geräten wird darauf verzichtet, da die benötigte Anpassung nur minimal ist.

Der Zugriff auf die gesammelten Logs soll über ein Webinterface erfolgen. Der Zugriff soll verschlüsselt über HTTPS erfolgen. Dieses muss zwingend mit einem Benutzernamen und Passwort geschützt werden. Es soll dazu das „lwb.ch“ Domänenlogin verwendet werden können. Wichtig ist dabei, dass ein Zugriffskonzept erstellt wird, welches die Benutzung des installierten Systems nur für die Mitarbeiter des RI der TF Bern erlaubt.



In einem ersten Schritt werden nur Systemlogs gesammelt. In einem Nachfolgeprojekt ist es geplant, den Logversand auch für applikationsspezifische Logs einzurichten.

Damit die gesammelten Logs einfacher durchsucht werden können, werden Streams hinzugefügt, welche die eingegangenen Nachrichten nach selbst definierten Kriterien gruppieren.

Weiter wird Graylog 2 an Icinga gekoppelt. Auf diese Weise ist es möglich, Alarme aufgrund von aufgetretenen Logs zu versenden. Im Rahmen dieser IPA werden drei Alarmtrigger zu Demozwecken erstellt. Weitere Alarmtrigger machen vor allem bei applikationsspezifischen Logs Sinn, dessen Versand jedoch nicht Umfang dieses Projekts ist.

## 17.2 Vorgehensziele

Die Vorgehensziele sind während dem Projektablauf zu erfüllen, haben aber keinen Einfluss auf die Funktionalität des Produktes am Projektende.

Ziel ID	Ziel	Beschrieb
V1	Hermes 5 verwendet	Die Projektmethode Hermes 5 wird angewendet.
V2	Zeitplan eingehalten	Der Zeitplan wird eingehalten.
V3	Pro Tag ein Arbeitsjournal	Es wird pro Tag ein Arbeitsjournal geführt.
V4	Pünktlicher Upload der Arbeit	Die Arbeit ist am 27.02.15, 13:00 als PDF auf PkOrg hochgeladen.
V5	Pünktlicher Versand der Arbeit	Die Arbeit ist am 27.02.15 per Post an die Experten verschickt
V6	Pünktliche Abgabe des Websummary	Das Websummary ist am 05.03.15 auf PkOrg hochgeladen
V7	Arbeitsort – TF Bern	Die Arbeit wird in der Technischen Fachschule Bern durchgeführt.
V8	Abschluss Initialisierungsphase	Die Initialisierungsphase soll am 11.02.15 abgeschlossen sein.
V9	Abschluss Konzeptphase	Die Konzeptphase soll am 16.02.15 abgeschlossen sein.
V10	Abschluss Realisierungsphase	Die Realisierungsphase soll am 23.02.15 abgeschlossen sein.

Tabelle 23: Vorgehensziele

## 17.3 Systemziele

Die Systemziele definieren, was am Ende des Projektes alles erfüllt sein muss.

Ziel ID	Ziel	Beschrieb
S1	Graylog ist installiert	Graylog Server und Web ist inklusive den Abhängigkeiten (Elasticsearch, MongoDB, Logstash) installiert und konfiguriert.
S2	Nginx ist installiert	Nginx ist zu Verwendung als Reverse Proxy konfiguriert.
S3	Zugriff auf Graylog ist geregelt	Der Zugriff ist gemäss dem Zugriffskonzept konfiguriert und funktioniert wie geplant.
S4	Logstash ist installiert	Logstash installiert und konfiguriert.
S5	Systemdokumentation ist vorhanden	Es liegt eine Systemdokumentation vor.
S6	Backup eingerichtet	Das Backup für den Logserver ist installiert
S7	Monitoring eingerichtet	Das Monitoring ist gemäss Monitoring-Konzept konfiguriert.
S8	Sendende Host konfiguriert	Die Logs sendenden Host sind konfiguriert.
S9	Streams eingerichtet	Unter Graylog sind die benötigten Streams zur einfacheren Auswertung erfasst.
S10	Script vorhanden	Ein Script zum automatischen Hinzufügen von Logs sendenden Windows und Linux Server ist vorhanden.

**Tabelle 24: Systemziele**

## 17.4 Anforderungen

### 17.4.1 Funktionale Anforderungen

Die funktionalen Anforderungen beschreiben gewünschte Funktionalitäten des Systems (Sollzustand) sowie dessen Daten und Verhalten.

Anforderung ID	Anforderung	Beschrieb
F1	Logs speichern	Der Logserver kann Nachrichten empfangen, normalisieren und speichern.
F2	Logs anzeigen	Über das Graylog Webinterface können gesammelte Nachrichten angezeigt werden.
F3	Logs durchsuchen	Über das Graylog Webinterface können gesammelte Nachrichten durchsucht werden.
F4	Webinterface-Zugriff verschlüsselt	Der Zugriff auf das Graylog Webinterface erfolgt verschlüsselt über HTTPS.
F5	Backup des Logservers	Es wird ein tägliches Backup der Konfigurationsdateien des Logservers angelegt.
F6	Monitoring eingerichtet	Die Systemdienste des Logservers sowie die Dienste, welche für das Logmanagement verwendet werden, werden durch die bestehende Icinga Installation überwacht.
F7	Installationsscript erstellt.	Zur Installation und Konfiguration benötigter Dienste auf den Log sendenden Windows und Linux Server wird ein Script erstellt, welche die benötigten Änderungen automatisch vornimmt.



F8	Authentifizierung Webinterface	Der Zugriff auf das Webinterface wird durch eine Authentifizierung mit Benutzername und Passwort geschützt. Als Zugangsdaten muss das gewohnte „lwb.ch“ Domänenlogin verwendet werden können.
F9	Autorisierung Webinterface	Der Zugriff auf das Webinterface ist nur für Mitarbeiter des Ressorts Informatik der TF Bern erlaubt. Dies wird über eine globale Gruppe der Domäne „lwb.ch“ umgesetzt.
F10	Graylog Stream für OS	Im Graylog wurden Streams eingerichtet. Diese teilen die Lognachrichten nach Betriebssystem des Senders auf.
F11	Graylog Stream für DFSR	Da in der letzten Zeit vermehrt Probleme mit der Distributed File System Replication (DFSR) auf den Domänencontroller aufgetreten sind, wurde dafür ein Stream angelegt.
F12	Beispiel Alarme	Für Demozwecke sind 3 Alarme/Alarmtrigger zu Demozwecken angelegt.
F13	Dashboard	Im Webinterface ist ein Dashboard angelegt worden, welches einem einen schnellen Überblick über den aktuellen Systemstatus zurückgibt.
F14	Windows Server hinzugefügt	Die nachfolgenden Linux Server senden die Logs an den zentralen Logserver: <ul style="list-style-type: none"><li>• PHLIC1</li><li>• PHBACKUP1</li><li>• VMDB1</li><li>• VMDC1</li><li>• VMDC2</li><li>• VMDC3</li><li>• VMDC4</li><li>• VMDC5</li><li>• VMDIENST1</li><li>• VMFSL1</li><li>• VMFSS1</li><li>• VMFSV1</li><li>• VMIS1</li><li>• VMMAIL1</li><li>• VMORGA1</li><li>• VMPRINT1</li></ul>
F15	Linux Server hinzugefügt	Die nachfolgenden Linux Server senden die Logs an den zentralen Logserver: <ul style="list-style-type: none"><li>• VMFILE1</li><li>• VMMON1</li><li>• VMRM1</li><li>• VMWEB1</li><li>• PHDR1</li></ul>
F16	Netzwerk-komponenten hinzugefügt	Die nachfolgenden Switches senden die Logs an den zentralen Logserver: <ul style="list-style-type: none"><li>• lo003-o01aa-sd1</li><li>• lo003-o01aa-sa3</li><li>• lo003-o01aa-sa4</li><li>• lo003-o01ba-sa1</li><li>• lo003-u01aa-sa1</li><li>• lo003-u01aa-sa2</li><li>• lo003-o01da-sa1</li></ul>



		<ul style="list-style-type: none"><li>• lo003-o01da-sa2</li><li>• lo003-e00aa-sa1</li><li>• lo003-o03aa-sa1</li><li>• lo003-o02aa-sa1</li><li>• lo003-o02aa-sa2</li><li>• lo003-e00ba-sa1</li><li>• lo003-e00ba-sa2</li><li>• lo003-o01ca-sa1</li><li>• lo003-o01ca-sa2</li><li>• lo01b-u01aa-sa1</li><li>• lo01b-u01ba-sa1</li><li>• lo01b-u01ca-sa1</li><li>• lo01b-u01da-sa1</li><li>• lo01b-u02aa-sa1</li><li>• fe017-u01aa-sd1</li><li>• fe017-e00aa-sa1</li><li>• fe017-u01aa-sa2</li><li>• fe017-o01aa-sa1</li><li>• fe017-e00ba-sa1</li><li>• fe017-e00fa-sa1</li><li>• fe017-o01ba-sa1</li><li>• fe017-o01ba-sa2</li><li>• fe017-o02aa-sa1</li><li>• fe017-e00da-sa1</li><li>• fe017-e00ea-sa1</li><li>• fe017-e00ca-sa1</li></ul>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabelle 25: Funktionale Anforderungen

#### 17.4.2 Nicht funktionale Anforderungen

Anforderung ID	Anforderung	Beschrieb
NF1	Installations- und Konfigurationsdokumentation	Die Installation und Konfiguration der Software wird dokumentiert.
NF2	Zugriff auf Webinterface max. 5 Sekunden	Der Zugriff auf die Loginmaske, das Dashboard oder die Suchfunktion im Webinterface dauern maximal 5 Sekunden.
NF3	Installationsprobleme dokumentiert	Die Probleme während der Installation und Konfiguration sind dokumentiert.
NF4	Testprotokoll vorhanden	Von den durchgeführten Tests wird ein Testprotokoll angelegt.

Tabelle 26: Nicht funktionale Anforderungen

## 17.5 Risikoanalyse

Mit Hilfe der Risikoanalyse werden die Risiken und dessen Auswirkungen aufgezeigt. Nachfolgend ist eine Tabelle mit den potentiellen Risiken und deren Schadensausmassen und Eintrittswahrscheinlichkeiten, sowie Schadensausmasse und Eintrittswahrscheinlichkeiten nach dem Ergreifen der Massnahme ersichtlich. Die Legende für das Schadensausmass und die Eintrittswahrscheinlichkeit sind auf der nächsten Seite zu finden.

Nr.	Risikobeschreibung	Auswirkung	Vor Massnahme		Massnahmen	Nach Massnahme	
			Schadensausmass	Eintrittswahrscheinlichkeit		Schadensausmass	Eintrittswahrscheinlichkeit
R1	Zeit reicht nicht aus	Das Projekt kann nicht pünktlich fertiggestellt werden.	S3	W3	Erstellen eines guten Zeitplans mit genügend Reserven.	S3	W2
R2	Konfigurationsfehler	Durch einen Konfigurationsfehler funktioniert die Software auf dem Logserver oder einem der sendenden Hosts nicht ordnungsgemäss.	S3	W2	Sämtliche Konfigurationsdateien werden vor jeder Änderung gesichert.	S2	W2
R3	Datenverlust	Die Dokumentation kann nicht fortgeführt werden.	S4	W2	Das Backup der TF Bern Daten, welches gemäss dem Backupkonzept täglich durchgeführt wird. Stellt sicher, dass die Daten bei Verlust auch wiederhergestellt werden können.	S2	W2
R4	Krankheit/Unfall	Die IPA kann nicht pünktlich abgeschlossen werden.	S4	W2	Bei einer auftretenden Krankheit oder einem Unfall wird unverzüglich der IPA Hauptexperte informiert. Anschliessend wird das weitere Vorgehen besprochen.	S1	W2
R5	Systemausfall	Aufgrund eines Systemausfalls kann die IPA nicht fortgeführt bzw. nicht pünktlich abgeschlossen werden.	S4	W2	Bei einem auftretenden Systemausfall wird unverzüglich der IPA Hauptexperte informiert. Anschliessend wird das weitere Vorgehen besprochen.	S2	W2
R6	Konfiguration eines senden Hosts nicht möglich	Aufgrund eines Fehlers, der bei einem Host auftritt, welcher die Lognachrichten an den zentralen Server senden soll, kann dieser nicht ordnungsgemäss konfiguriert werden.	S2	W4	Es wird genügend Zeit für die Installation und Konfiguration der sendenden Hosts eingeplant. Auf diese Weise kann auf ein mögliches Problem reagiert werden.	S1	W4

Tabelle 27: Risikoanalyse



## 17.5.1 Legende

### 17.5.1.1 Schadensausmass

Abkürzung	Beschrieb
<b>S1</b>	führt zu keiner Abwertung
<b>S2</b>	geringe Abwertung bis 1.0 Notenpunkte
<b>S3</b>	hohe Abwertung über 1,0
<b>S4</b>	führt zu Nichtbestehen

Tabelle 28: Schadensausmass

### 17.5.1.2 Eintrittswahrscheinlichkeit

Abkürzung	Beschrieb
<b>W1</b>	unvorstellbar
<b>W2</b>	unwahrscheinlich
<b>W3</b>	eher vorstellbar
<b>W4</b>	wahrscheinlich
<b>W5</b>	sehr wahrscheinlich

Tabelle 29: Eintrittswahrscheinlichkeit

## 17.6 Risikograph

### 17.6.1 Vor Massnahmen

Der nachfolgende Risikograph zeigt die Risiken vor dem Ergreifen der Massnahmen.

Eintrittswahrscheinlichkeit	sehr wahrscheinlich				
	wahrscheinlich		R6		
	eher vorstellbar			R1	
	unwahrscheinlich			R2	R3, R4, R5
	unvorstellbar				
		führt zu keiner Abwertung	geringe Abwertung bis 1.0 Notenpunkte	hohe Abwertung über 1,0	führt zu Nichtbestehen
		Schadensausmass			

Tabelle 30: Risikograph - vor Massnahmen



## 17.6.2 Nach Massnahmen

Der nachfolgende Risikograph zeigt die Risiken nach Ergreifen der Massnahmen.

Eintrittswahrscheinlichkeit	sehr wahrscheinlich				
	wahrscheinlich	R6			
	eher vorstellbar				
	unwahrscheinlich	R4	R2, R3, R5	R1	
	unvorstellbar				
		führt zu keiner Abwertung	geringe Abwertung bis 1.0 Notenpunkte	hohe Abwertung über 1,0	führt zu Nichtbestehen
		Schadensausmass			

Tabelle 31: Risikograph - nach Massnahmen

## 18. Konzept

### 18.1 Logserver Konzept

Das nachfolgende Unterkapitel zeigt das Konzept des eigentlichen Logservers auf. Weiter wird auf die Architektur und des Datenflusses unter den einzelnen Diensten eingegangen.

#### 18.1.1 Systemarchitektur

Die nachfolgende Grafik zeigt die geplante Kommunikation zwischen den einzelnen Diensten.

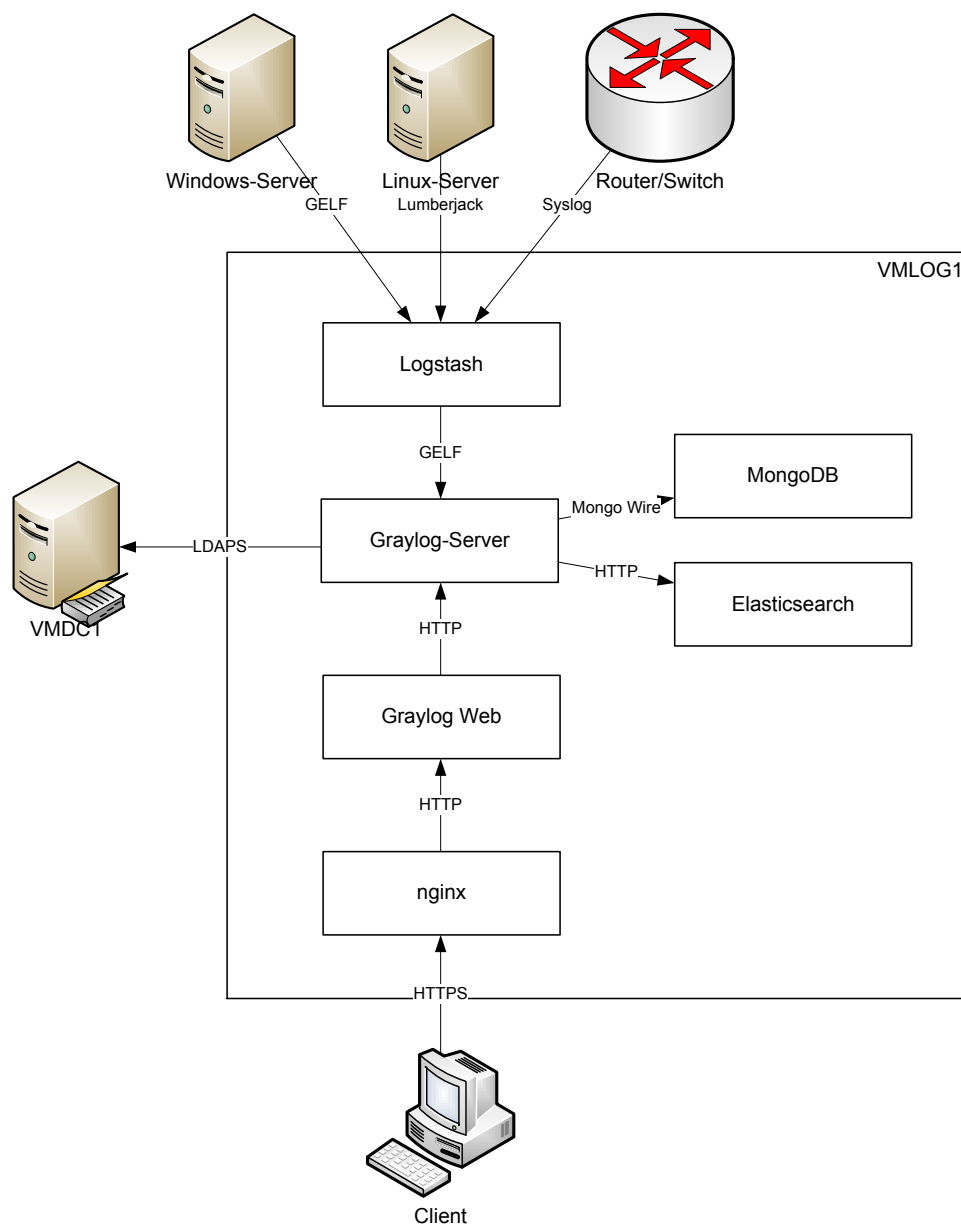


Abbildung 5: Systemarchitektur

### 18.1.2 Erläuterung der verwendeten Dienste

Die nachfolgende Tabelle zeigt auf, welche Dienste auf dem Logserver (VMLOG1) installiert werden und für was sie verwendet werden.

Dienst	Beschrieb
Elasticsearch	Elasticsearch ist ein Datenspeicher, welcher von Graylog verwendet wird. Er wird über HTTP angesprochen und stellt eine REST Schnittstelle bereit. Graylog legt darin alle empfangenen Lognachrichten ab. Auf eine Authentifizierung und Verschlüsselung kann verzichtet werden, da der Dienst an das Loopback-Interface von VMLOG1 gebunden wird.
MongoDB	MongoDB wird von Graylog als Datenspeicher für die aktuelle Konfiguration verwendet. MongoDB ist eine dokumentenorientierte NoSQL Datenbank. Achtung: Entgegen der weit verbreiteten Information nutzt die aktuelle Graylog Version MongoDB nicht mehr als Speicher für Lognachrichten. MongoDB wird über TCP/IP das eigens entwickelte Mongo Wire Protokoll angesprochen. Auf eine Authentifizierung und Verschlüsselung kann verzichtet werden, da der Dienst an das Loopback-Interface von VMLOG1 gebunden wird.
Logstash	Logstash ist ein Open Source Produkt, welches in diesem Fall zur Lognormalisierung genutzt wird. Über mehrere Inputs werden Lognachrichten empfangen, anschliessend normalisiert und schliesslich an einen anderen Dienst, in diesem Fall an den Graylog Server, weitergeleitet. Die Art der Authentifizierung und Verschlüsselung ist von der Art des verwendeten Inputs abhängig.
Graylog Server	Graylog Server empfängt die Logs von Logstash, verarbeitet sie durch mehrere Filter Chains und legt sie in Elasticsearch ab. Weiter stellt es eine REST Schnittstelle die Suche und Anzeige der Logs zur Verfügung. Die Authentifizierung geschieht mit Hilfe von lokalen Benutzern, sowie einer LDAP Schnittstelle auf das Active Directory der Domäne „lwb.ch“. Der Zugriff auf den Graylog Server ist nicht verschlüsselt. Da sich das Webinterface jedoch auf demselben Server befindet, kann die Verbindung nicht mitgehört werden.
Graylog Web	Graylog Web ist das eigentliche Webinterface von Graylog. Über dieses können Logs durchsucht und angezeigt werden. Weiter sind grundlegende Konfigurationsänderungen möglich. Die Daten werden vom Graylog Server Dienst bezogen. Die Authentifizierung geschieht ebenfalls direkt auf dem Graylog Server. Da eine Verschlüsselung mit Graylog Web nur eingeschränkt möglich ist, wird nginx als Reverse Proxy davor geschaltet, damit dieser die Verschlüsselung von des HTTP Traffics mithilfe TLS/SSL übernehmen kann.
nginx	nginx fungiert in dieser Architektur lediglich als Reverse Proxy, um den Datenverkehr zwischen Client und dem Server VMLOG1 verschlüsseln zu können.

**Tabelle 32: Erläuterung der verwendeten Dienste**

### 18.1.3 Erläuterung der verwendeten Protokolle

Die nachfolgende Tabelle zeigt auf, welche Protokolle von der geplanten Systemarchitektur genutzt werden.

Protokoll	Beschrieb
HTTP	Verwendung: Website-Content TCP/UDP: TCP Standard-Dest.-Port: 443 Verschlüsselung: keine
HTTPS	Verwendung: Website-Content TCP/UDP: TCP Standard-Dest.-Port: 443 Verschlüsselung: SSL/TLS
LDAPS	Verwendung: LDAPS TCP/UDP: TCP Standard-Dest.-Port: 636 Verschlüsselung: SSL/TLS
Lumberjack	Verwendung: Logging nach Wahl TCP/UDP: nicht standardisiert Standard-Dest.-Port: SSL/TLS Verschlüsselung:
Syslog	Verwendung: Logging nach Wahl TCP/UDP: 514 Standard-Dest.-Port: keine Verschlüsselung:
GELF	Verwendung: Logging nach Wahl TCP/UDP: 12201 Standard-Dest.-Port: keine Verschlüsselung:
Mongo Wire	Verwendung: MongoDB TCP/UDP: TCP Standard-Dest.-Port: 27017 Verschlüsselung: keine

**Tabelle 33: Erläuterung der verwendeten Protokolle**

#### 18.1.4 Service Schnittstellen

Die nachfolgende Tabelle zeigt die Abhängigkeiten unter den einzelnen Services.

Abhängig Von Service	Logstash	Graylog-Server	Graylog-Web	Nginx	MongoDB	Elasticsearch
Logstash		X				
Graylog-Server					X	X
Graylog-Web		X				
Nginx			X			
MongoDB						
Elasticsearch						

Tabelle 34: Service Schnittstellen

#### 18.1.5 Netzwerk Konfiguration Logserver

Als Netzwerkkonfiguration des Logservers sind die nachfolgenden Einstellungen vorgesehen.

Attribut	Wert
VLAN	Service
Hostname	VMLOG1
Domäne	lwb.ch
IP-Adresse	86.118.120.30
Netzadresse	86.118.120.0
Broadcast	86.118.120.255
Gateway	86.118.120.1
DNS Server	86.118.120.170, 86.118.120.171

Tabelle 35: Netzwerk Konfiguration VMLOG1

#### 18.1.6 Netzübergreifende Kommunikation

Wichtig ist, dass sämtliche Lognachrichten sendenden Hosts Netzwerkzugriff auf VMLOG1 haben. Da in der TF Bern-Infrastruktur sämtliche VLAN's auf das Service-VLAN Zugriff haben, ist es nicht notwendig, für dieses Projekt zusätzliche Firewall Regeln zu erstellen.

### 18.1.7 Systemanforderungen VMLOG1

Da bei einer unzureichenden Performance eines Logservers die Wahrscheinlichkeit höher ist, dass Lognachrichten verloren gehen, ist es wichtig, die verfügbaren Ressourcen nicht zu knapp zu bemessen. Aus der Schätzung der benötigten Ressourcen des virtuellen Servers wurden folgende Anforderungen ausgearbeitet:

Komponente	Anforderung	Bemerkungen
RAM	4 GB	Da besonders Elasticsearch sehr viel Arbeitsspeicher verwendet, sind 4 GB das Minimum
CPU Kerne	2	
Festplatte 1	20 GB	System
Festplatte 2	75 GB	Die zweite Festplatte wird für die Speicherung der Daten von MongoDB und Elasticsearch verwendet. Vermutlich wird es in Zukunft mehr Speicher benötigen. Da der Speicher im SAN der TF Bern etwas knapp ist und ein Speicherausbau ansteht, werden vorerst nur die 75 GB zugewiesen
Netzwerk	1 Gbit/s	
CD Laufwerk	Ja	

**Tabelle 36: Systemanforderungen VMLOG1**

### 18.1.8 Inputs Logstash

Bei Logstash können mehrere Inputs eingerichtet werden. Damit das installierte Betriebssystem des Senders nicht mühsam und fehleranfällig automatisch erkannt werden muss, wird pro Betriebssystem bzw. Typ ein einzelner Input mit unterschiedlichem Port erstellt. Nach dem Empfangen der Nachricht wird sie mit einem Typen Tag versehen.

In der nachfolgenden Tabelle sind die geplanten Inputs ersichtlich:

Port	Protokoll	Bemerkungen
5000	Lumberjack	Input für Linux Sever
5001	GELF	Input für Windows Server
5002	Syslog	Input für Cisco Switches und Router

**Tabelle 37: Inputs Logstash**



### 18.1.9 Inputs Graylog

Auch bei Graylog können mehrere Inputs hinzugefügt werden. Da die Nachrichten aber schon durch Logstash normalisiert wurden, muss keine weitere Normalisierung vorgenommen werden. Aus diesem Grund wird nur der nachfolgende Input eingerichtet.

Port	Protokoll	Bemerkungen
12201	GELF	Input für alle von Logstash weitergeleiteten Nachrichten

Tabelle 38: Inputs Graylog

### 18.1.10 Filter Logstash

Unter Logstash werden die nachfolgenden Filter zur Lognormalisierung eingerichtet:

- Linux-Syslog
- Windows-EventLog
- Cisco-Syslog

### 18.1.11 Extractor Graylog

Extractor unter Graylog sind ungefähr dasselbe wie Filter unter Logstash. Da die Normalisierung durch Logstash durchgeführt wird, werden keine Extractor unter Graylog konfiguriert.

### 18.1.12 Outputs Logstash

Unter Logstash wird lediglich ein Output eingerichtet, welcher die normalisierten Nachrichten an Graylog weitersendet. Dieser wird auf die nachfolgende Weise konfiguriert:

Host	Protokoll	Port	Bemerkungen
127.0.0.1	GELF	12201	Input für alle von Logstash normalisierten Nachrichten

Tabelle 39: Outputs Logstash

### 18.1.13 Outputs Graylog

Unter Graylog werden keine Outputs konfiguriert, da die Logs nach der Speicherung nicht mehr weitergeleitet werden können.

### 18.1.14 Graylog Streams

Unter Graylog können Streams angelegt werden, um die Nachrichten besser und einfacher durchsuchen zu können. Weiter werden sie zum Erstellen von Alarmierungen verwendet. Im Gegensatz zu den gespeicherten Searches, sind die Streams in Echtzeit. Im Rahmen der IPA werden die nachfolgenden Streams erstellt.

Name	Bedingung	Bemerkungen
Windows	OS entspricht Windows	Nachrichten aller Windows Server
Linux	OS entspricht Linux	Nachrichten aller Linux Server
Cisco	OS entspricht Cisco IOS	Nachrichten aller Cisco Geräte
DFSR Fehler	Log entspricht ungültiger DFS Replication	Nachrichten welche anzeigen, dass ein Problem mit der DFS Replication besteht
Ungültige SSH Logins	Log entspricht ungültigem SSH Login	Nachrichten welche anzeigen, dass ein Loginversuch mit ungültigen Daten stattgefunden hat. Dieser Stream dient zu Beispielzwecken.
Windows Server Crash Shutdown	Event ID entspricht 41	Nachrichten welche anzeigen, dass ein Windows Server unsauber herunter gefahren wurde.

**Tabelle 40: Graylog Streams**

### 18.1.15 Graylog Alerts

Unter Graylog können Alerts ausgelöst werden, wenn eine bestimmte Anzahl von Nachrichten, in einer bestimmten Zeit in einem Stream empfangen werden. Die Auslösung kann über ein Icinga bzw. Nagios Plugin überprüft werden. Die Alarme machen vor allem in Systemen Sinn, in welchen eigens entwickelte Applikationen laufen, bei welchen Performance Daten oder ähnliches überprüft werden. Da dies in der Umgebung der TF Bern nicht der Fall ist, werden lediglich die nachfolgenden Alarme zu Demozwecken erstellt:

Name	Bedingung	Bemerkungen
DFSR Fehler	Anzahl Nachrichten im Stream „DFSR Fehler“ > 5 in der letzten Stunde	Zeigt an, dass ein Problem mit der DFS Replication besteht.
Ungültige SSH Logins	Anzahl Nachrichten im Stream „Ungültige SSH Logins“ > 5 in der letzten Stunde	Zeigt an, dass vermehrt Loginversuche mit ungültigen Daten stattgefunden haben. Dieser Stream dient zu Beispielzwecken.
Windows Server Crash Shutdown	Anzahl Nachrichten im Stream „Windows Server Crash Shutdown“ > 1 in der letzten Stunde	Zeigt an, dass ein Windows Server unsauber herunter gefahren wurde.

**Tabelle 41: Graylog Alerts**





## 18.1.16 Logversand

In den nachfolgenden Unterkapiteln ist aufgezeigt, auf welche Art und Weise, die sendenden Hosts, welche Logs, an VMLOG1 weitersenden. Bei sämtlichen Protokollen wird auf die UDP Variante zurückgegriffen, da bei einer Software, welche das Logging schlecht implementiert hat, enorme Performanceeinbußen bei Verwendung der TCP Variante entstehen können. Weiter wird beim empfangenden Host immer eine IP Adresse, mit Ausnahme von Lumberjack, anstelle einem FQDN verwendet, damit der Versand auch bei Auftreten eines DNS-Problems gewährleistet ist. Bei Lumberjack muss aufgrund der Zertifikatsauthentifizierung zwingend ein Name genutzt werden.

### 18.1.16.1 Linux Server

<b>Verwendete Software</b>	Logstash-Forwarder
<b>Dateien/Kriterien</b>	<ul style="list-style-type: none"><li>• /var/log/messages</li><li>• /var/log/auth.log</li><li>• /var/log/mail.info</li><li>• /var/log/mail.err</li><li>• /var/log/mail.warn</li><li>• /var/log/syslog</li></ul>
<b>Empfangender Host</b>	log.lwb.ch
<b>Port</b>	5000
<b>Protokoll</b>	Lumberjack UDP

Tabelle 42: Logversand - Linux Server

### 18.1.16.2 Windows Server

<b>Verwendete Software</b>	NXLog
<b>Dateien/Kriterien</b>	Gesamtes Windows Eventlog
<b>Empfangender Host</b>	86.118.120.30 (VMLOG1)
<b>Port</b>	5001
<b>Protokoll</b>	GELF UDP

Tabelle 43: Logversand - Windows Server

### 18.1.16.3 Switches und Router

<b>Verwendete Software</b>	Bordmittel
<b>Dateien/Kriterien</b>	Gesamtes Systemlog ab Loglevel Debug
<b>Empfangender Host</b>	86.118.120.30 (VMLOG1)
<b>Port</b>	5002
<b>Protokoll</b>	Syslog UDP

Tabelle 44: Logversand - Switches und Router

## 18.1.17 Installationsscript

Zur Installation und Konfiguration der sendenden Linux und Windows Server wird ein Script erstellt. Das Script soll Logstash-Forwarder bzw. NXLog installieren, die notwendige Konfiguration vornehmen und den Dienst neu starten. Das Script wird vor der Verwendung auf den produktiven Servern auf einer unproduktiven VM getestet.

### 18.1.18 Dashboards

Im Rahmen dieses Projekts wird in Graylog eine Dashboard erstellt, welches den Mitarbeitenden des RI einen schnellen Überblick über den aktuellen Logstatus geben soll. Geplant ist eine Darstellung, wie in der nachfolgenden Grafik ersichtlich.

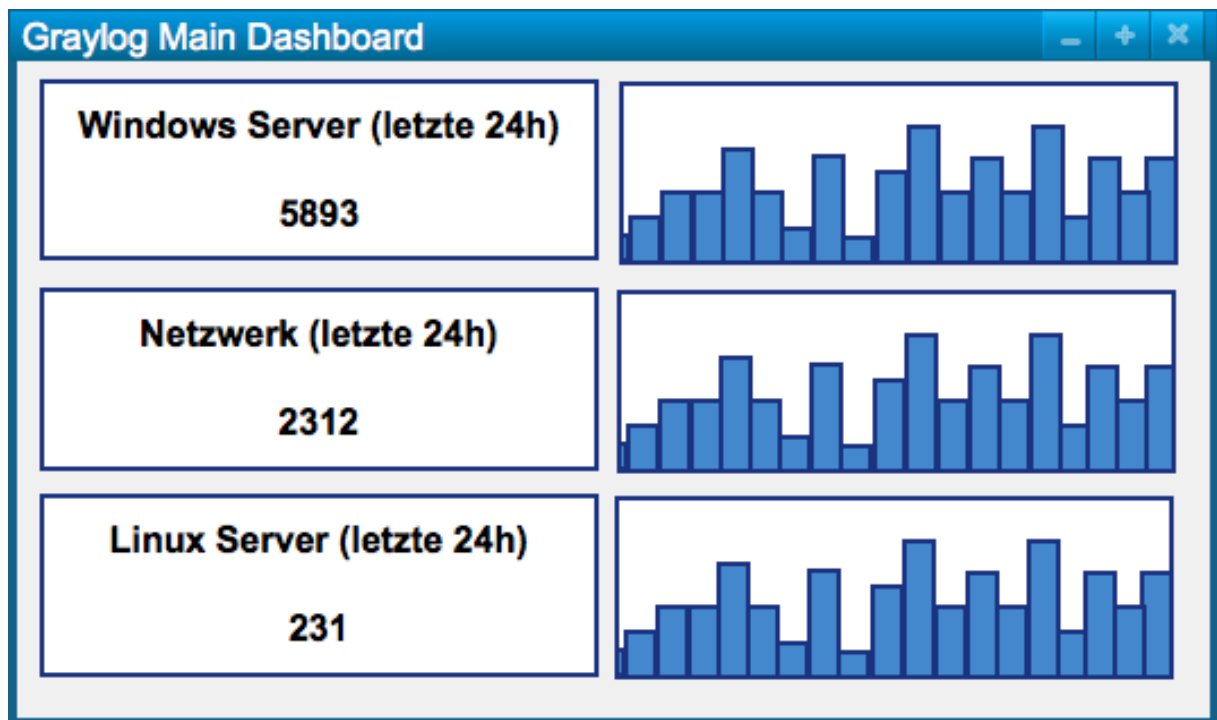


Abbildung 6: Graylog Dashboard

### 18.1.19 Grundinstallation VMLOG1

Die Grundinstallation des Server VMLOG1 erfolgt gemäss „Standardinstallation Linux“ (Seite 135).

### 18.1.20 Zu installierende Software (VMLOG1)

Die nachfolgende Tabelle zeigt auf, welche Software auf dem Server VMLOG1 installiert werden muss, zudem deren Quelle und zu welcher Software eine Abhängigkeit (Anforderung) besteht, welche nicht automatisch behoben wird (durch Paketmanager). Falls keine Version angegeben wird, ist die aktuellste, verfügbare Version zu installieren.

Name	Abhängigkeit	Quelle	Bemerkungen
Archey	-	Debian Repo	Zur Anzeige des Systemstatus beim Login
Duplicity	-	Debian Repo	Abhängigkeit zu Backupsript



Elasticsearch	Java	Elasticsearch Repo	
Graylog Server	Java	Graylog Repo	
Graylog Web	Java	Graylog Repo	
Java 8	-	PPA	Es wird die Oracle Java Version verwendet, da in der Vergangenheit schlechte Erfahrungen mit dem OpenJDK gemacht wurden.
Logstash	Java	Elasticsearch Repo	
Logstash Forwarder	-	Elasticsearch Repo	Verschicken der eigenen Systemlogs
MongoDB	-	Mongo Repo	Auch im Debian Repository ist eine MongoDB Version verfügbar. Diese ist jedoch nicht mehr aktuell.
Nagios NRPE Server	-	Debian Repo	Monitoringclient
Nginx	-	Debian Repo	Zur Verwendung als Reverse Proxy
OpenSSH-Server	-	Debian Repo	Für SSH Zugriff
Postfix	-	Debian Repo	Zum Mailversand des Backupstatus
VMWare Tools	-	VMWare	

Tabelle 45: Zu installierende Software (VMLOG1)

### 18.1.21 Zugriff Logserver

Damit der Zugriff auf den Logserver etwas einfacher wird, werden die folgenden Einträge in der internen DNS Zone „lwb.ch“ erstellt. Bei sämtlichen A Records wird ebenfalls der zugehörige Eintrag in der Reverse Lookup Zone erstellt.

vmlog1	IN A	86.118.120.30
log	IN CNAME	vmlog1

## 18.2 Namenskonzept

Eigentlich ist das Namenskonzept nicht Teil dieser IPA. Leider ist jedoch das bestehende Namenskonzept aufgrund einer kürzlich erfolgten Migration nicht mehr aktuell. Daher sind in den nachfolgenden Unterkapiteln das angepasste Namenskonzept für Server und Netzwerkkomponenten ersichtlich.

### 18.2.1 Server

Der Hostname eines Servers setzt sich aus den nachfolgenden Bestandteilen zusammen:

[Typ][Zweck][Nummer]



#### 18.2.1.1 Typ

Der Typenteil, zeigt ob ein Server virtuell oder physikalisch ist.

Abkürzung	Bedeutung
PH	Physikalischer Server
VM	Virtueller Server

Tabelle 46: Namenskonzept - Server - Typ

#### 18.2.1.2 Zweck

Der zeigt an, für welchen Zweck ein Server verwendet wird.

Abkürzung	Bedeutung
BACKUP	Backupserver
DB	Datenbankserver
DC	Domaincontroller
DIENST	Allgemeine Dienste
DR	Datenspiegelungsserver
FILE	File Zugriff von Zuhause
FS	Fileserver
IS	Informationssystem
LIC	Lizenzserver
LOG	Logserver
MON	Monitoring Server
ORGA	Orgamax-Server
PRINT	Printserver
RM	Redmine Server
WEB	Webserver

Tabelle 47: Namenskonzept - Server - Zweck

#### 18.2.1.3 Nummer

Der Nummern-Teil des Hostnamens entspricht einer fortlaufenden Nummer.

#### 18.2.1.4 Beispiele

Die nachfolgende Tabelle zeigt einige Beispiele für Server Hostnamen.

Hostname	Bedeutung
VMDC3	3. virtueller Domaincontroller
VMWEB1	1. virtueller Webserver
PHLIC1	1. physikalischer Lizenzserver

Tabelle 48: Namenskonzept - Server - Beispiele



## 18.2.2 Netzwerkkomponenten

Das Namenskonzept für Netzwerkkomponenten wurde bei der Übernahme des Netzwerks von der Firma Connectis bzw. SPIE ICS übernommen. Es setzt sich aus den nachfolgenden Bestandteilen zusammen:

[Standort]-[Stockwerk][Rack]-[Typ][Nummer]

### 18.2.2.1 Standort

Der Standortteil steht für den Gebäudestandort.

Abkürzung	Bedeutung
lo003	Lorraine Hauptgebäude
lo01b	Lorraine Shed
fe017	Felsenau

Tabelle 49: Namenskonzept - Netzwerkkomponenten - Standort

### 18.2.2.2 Stockwerk

Der Stockwerkteil steht für das Stockwerk der Netzwerkkomponente

Abkürzung	Bedeutung
e00	Erdgeschoss
o01	1. Obergeschoss
o02	2. Obergeschoss
o03	3. Obergeschoss
u01	1. Untergeschoss
u02	2. Untergeschoss

Tabelle 50: Namenskonzept - Netzwerkkomponenten - Stockwerk

### 18.2.2.3 Rack

Der Rackteil steht für den Identifier des Racks in diesem Stockwerk und wird mit zwei Buchstaben gekennzeichnet. Der Bezeichner geht von „aa“, „ab“, „ac“ über „az“ bis „zz“.

### 18.2.2.4 Typ

Der Typenteil steht für den Typ der Netzwerkkomponente.

Abkürzung	Bedeutung
sa	Access Switch
sd	Distribution Switch

Tabelle 51: Namenskonzept - Netzwerkkomponenten - Typ

### 18.2.2.5 Nummer

Der Nummern Teil des Hostnamens entspricht einer fortlaufenden Nummer.

### 18.2.2.6 Beispiele

Die nachfolgende Tabelle zeigt einige Beispiele für Hostnamen von Netzwerkkomponenten.

Hostname	Bedeutung
lo003-o01aa-sd1	1. Distribution Switch im 1. Rack im 1. Stock im Lorraine Hauptgebäude
lo003-e00ba-sa2	2. Access Switch im 2. Rack im Erdgeschoss im Lorraine Hauptgebäude
lo01b-u02aa-sa1	1. Access Switch im 1. Rack im 2 Untergeschoss des Lorraine Sheds

**Tabelle 52: Namenskonzept - Netzwerkkomponenten - Beispiele**

## 18.3 Monitoring-Konzept

Bei der TF Bern wird das Monitoring mit Icinga 1 durchgeführt. Der Logserver soll im Rahmen dieses Projekts ebenfalls in das Monitoringsystem aufgenommen werden, damit sichergestellt werden kann, dass er ständig erreichbar ist und eventuell auftretende Probleme im laufenden Betrieb zeitnah erkannt und behoben werden können.

### 18.3.1 Checks VMLOG1

Es ist geplant, dass folgende Checks vom Icinga-Server (VMMON1) auf dem Logserver (VMLOG1) durchgeführt werden.

Name	Warnschwelle	Kritische Schwelle	Beschrieb
Ping	keine	keine	Host wird als Down angezeigt, wenn der Pingrequest keine Antwort zurückliefert
Load	15,10,5	30,25,20	Liefert den aktuellen Systemload zurück
Angemeldete Benutzer	5	10	Prüft die Anzahl angemeldeter Benutzer
Disk Nutzung	80%	100%	Überprüft den genutzten Speicherplatz
HTTP	-	> 10s	Überprüft ob der Server über HTTP erreicht werden kann.
HTTPS	-	> 10s	Überprüft ob der Server über HTTPS erreicht werden kann.
Packet Loss	10%	80%	Überprüft die Anzahl von verlorenen Paketen bei mehreren hintereinander folgenden Pings
SSH	-	> 10s	Überprüft ob der Server über SSH erreicht werden kann.
Anzahl Prozesse	150	200	Überprüft die Anzahl Prozesse
MongoDB	-	> 10s	Überprüft die Verfügbarkeit des MongoDB Dienstes
Elasticsearch	-	> 10s	Überprüft die Verfügbarkeit des Elasticsearch Dienstes
Graylog Web	-	> 10s	Überprüft die Verfügbarkeit des Graylog Web Dienstes.



Graylog Alerts	-	> 1	Überprüft die aufgetretenen Graylog Alerts in den letzten 60min.
----------------	---	-----	------------------------------------------------------------------

Tabelle 53: Monitoring-Konzept - Checks VMLOG1

### 18.3.2 Checks sendende Windows Server

Da es wichtig ist, dass der NXLog Dienst, welcher die Lognachrichten unter Windows verschickt, auch wirklich läuft, wird dies mit Hilfe eines Icinga Checks überprüft. Sämtliche bestehenden Checks bleiben selbstverständlich unangetastet.

Name	Warnschwelle	Kritische Schwelle	Beschrieb
nxlog.exe gestartet	keine	Läuft nicht	Überprüft ob ein Prozess mit dem Namen nxlog.exe läuft.

Tabelle 54: Monitoring-Konzept - Checks sendende Windows Server

### 18.3.3 Checks sendende Linux Server

Da es wichtig ist, dass der Logstash-Forwarder Dienst, welcher die Lognachrichten unter Linux verschickt, auch wirklich läuft, wird dies mit Hilfe eines Icinga Checks überprüft. Sämtliche bestehenden Checks bleiben selbstverständlich unangetastet.

Name	Warnschwelle	Kritische Schwelle	Beschrieb
logstash-forwarder gestartet	keine	Läuft nicht	Überprüft ob ein Prozess mit dem Namen logstash-forwarder läuft.

Tabelle 55: Monitoring-Konzept - Checks sendende Linux Server

### 18.3.4 Checks sendende Netzwerkkomponenten

Da unter Cisco der Syslog Versand tief im System integriert ist und keine einfache Überprüfung möglich ist, wird auf einen zusätzlichen Check unter den Cisco Netzwerkkomponenten verzichtet.

### 18.3.5 Alarmierung

Wie bisher bereits konfiguriert, wird bei sämtlichen Icinga Statusänderungen ein Alarm an den #icinga-host bzw. #icinga-service Channel in den Slack Messenger der TF Bern gesendet. Weiter haben die MA der RI den Nagstamon Client auf ihren Computern installiert. Im Rahmen dieses Projekts sind keine Änderungen an den Icinga Alarmierungseinstellungen notwendig.

## 18.4 Berechtigungskonzept

Manchmal stehen in Lognachrichten sensitive Informationen. Aus diesem Grund ist ein gut funktionierendes Berechtigungskonzept unabdingbar. Glücklicherweise lässt sich Graylog mit einem Active Directory koppeln. Sämtliche Benutzer und Gruppen, welche zur Berechtigungsreglementierung benötigt werden, bestehen bereits.

### 18.4.1 Konfiguration in Graylog

In Graylog lassen sich die Berechtigungen über LDAP Queries bestimmen. Das Ziel der Zugriff für die lokale Gruppe „G\_MA-INF“ der Domäne lwb.ch zu erlauben. LDAP Benutzer sollen Administratorrechte auf dem Graylog Webinterface erhalten.

### 18.4.2 Testbenutzer

Zum Testen stehen die Benutzer „TEST-L“ und „TEST-V“ zur Verfügung. Diese müssen gegebenenfalls gemäss dem Testkonzept angepasst werden.

### 18.4.3 Mitglieder G\_MA-INF

Nachfolgend sind die Mitglieder der globalen Gruppe „G-MA-INF“ aufgelistet. Diese Benutzer erhalten Zugriff auf das Graylog Webinterface.

Benutzername	Vorname	Nachname
SHH	Hetem	Shaqiri
CIV	Ivan	Cosic
STA	Stübi	Aaron
IHRI	Rida	Ihihi
IMF	Felix	Imobersteg
ZER	Roman	Zesiger

Tabelle 56: Mitglieder G\_MA-INF

### 18.4.4 Physikalischer Zugriff (Serverraum)

Der Zutritt zum Serverraum ist nur den MA des RI sowie den MA des Hausdienstes gestattet.

## 18.5 Backupkonzept

Die nachfolgenden Kapitel beschreiben, welche Dateien des Servers VMLOG1 auf welche Art und Weise gesichert werden.





### 18.5.1 Art des Backups

In Kürze wird von der TF Bern die Backupsoftware Veeam eingeführt. Bis zu diesem Zeitpunkt, werden alle Linux Server mithilfe einem selbst erstellten Script gesichert. Diese Lösung hat sich bisher sehr bewährt und wird auch in diesem Projekt so umgesetzt.

### 18.5.2 Ziel

Das Backup soll über FTP auf den Host NAS1 geschrieben werden. Genauer gesagt in den Ordner <ftp://BACKUP@NAS1.lwb.ch/Backup/duplicity/vmlog1/>. Da sich dieses NAS ebenfalls im Serverraum in der Lorraine steht, wird dieses Backup täglich in den Serverraum in der Felsenau repliziert. Dies geschieht vollautomatisch und muss im Rahmen dieses Projekts nicht angepasst werden.

### 18.5.3 Zu sichernde Daten

Auf dem Server VMLOG1 sollen die nachfolgenden Verzeichnisse gesichert werden:

Pfad / Datei / Inhalt	Beschrieb
/etc	Sicherung des Verzeichnis, in welchem sich Konfigurationsdateien befinden
/root	Homeverzeichnis des Root-Benutzers
/home	Standard Homeverzeichnisse der neu angelegten Benutzer
Paketliste	Liste aller aktuell installierten Softwarepakete

**Tabelle 57: Zu sichernde Daten**

### 18.5.4 Backupjobs

Um das Backupscript zu starten, wird ein Cronjob verwendet. Das Script soll jede Nacht um 03:00 Uhr gestartet werden.

### 18.5.5 Aufbewahrungsdauer

Die Aufbewahrungsdauer für Backups des Servers beträgt 180 Tage

### 18.5.6 Backuptyp

Das Script soll alle 30 Tage ein Full Backup aller Dateien anlegen. An allen anderen Tagen wird ein inkrementelles Backup durchgeführt.



### 18.5.7 Benachrichtigung

Bei jedem Backup soll der Output des Scripts an die Mailadresse [informatik@tfbern.ch](mailto:informatik@tfbern.ch) versendet werden.

### 18.5.8 Verschlüsselung des Backups

Das Backup wird nicht verschlüsselt, da dies in der Vergangenheit zu erheblichen Problemen geführt hat.

### 18.5.9 Restore

Das Script soll ebenfalls über eine Restorefunktion verfügen, welche selbsterklärend sein soll.

## 18.6 ISDS Konzept

Für dieses Projekt gelten die Datenschutzbestimmungen der TF Bern. In den nachfolgenden Unterkapiteln werden Massnahmen zur Informationssicherheit und zum Datenschutz aufgezeigt.

### 18.6.1 Zugriff auf das TF Bern Netzwerk

Der Zugriff auf das TF Bern Netzwerk ist nur autorisierten Personen der TF Bern gewährt. Lokale Benutzer haben keinen Zugriff aufs Netzwerk. Alle Mitarbeitenden verfügen über einen Domänenbenutzer mit definierten Rechten.

Es dürfen keine privaten Geräte an das Netzwerk der TF Bern angeschlossen werden. Dies gilt jedoch nicht für das Besucher-WLAN.

### 18.6.2 Zugriff auf lokale Computer

An den lokalen Computer der TF Bern kann nur mit einem Domänenbenutzer angemeldet werden. Diese Benutzer werden über Active Directory vom RI der TF Bern verwaltet und sind durch komplexe Passwörter geschützt.

### 18.6.3 IPA Daten

Sämtliche Daten der IPA werden nur autorisierten Personen zur Verfügung gestellt. Die Daten werden täglich gesichert. Weitere Informationen Dazu sind im Kapitel Datensicherung der IPA (Seite 24) zu finden.



#### 18.6.4 Virenschutz

Der Server VMLOG1 wird nicht mithilfe eines Virenschutz gesichert, da die TF Bern bei Linux Server keinen zusätzlichen Schutz verwendet.

#### 18.6.5 Internetschutz

Ungewollte, verdächtige oder schädliche Seiten oder Dateien werden durch den Proxyserver des BEWAN's blockiert.

#### 18.6.6 Übertragung von Daten

Sensitive Daten werden nach Möglichkeit verschlüsselt übertragen.

### 18.7 Testkonzept

Im nachfolgenden Testkonzept wird beschrieben, welche Tests auf welche Art und Weise durchgeführt werden sollen. Es werden die Testobjekte, Testkategorie, Testarten, Testvoraussetzungen, Testdurchführung und die Testfälle beschrieben. Die in diesem Kapitel spezifizierten Tests werden später, am Ende der Realisierungsphase, durchgeführt und mit Hilfe eines Testprotokolls dokumentiert.

#### 18.7.1 Testobjekte

In der folgenden Tabelle sind die Testobjekte aufgelistet und beschrieben. Auf den genannten Testobjekten werden diverse Tests durchgeführt, um die Funktionalität des Systems zu testen.

ID	Objekt	Beschrieb
TO1	Logstash	Konfigurierte Logstash Installation
TO2	Graylog Server	Business Layer von Graylog
TO3	Graylog Web	Webinterface von Graylog
TO4	nginx	Reverse Proxy
TO5	Icinga	Monitoringsystem
TO6	Backupscript	Script zum Durchführen des Backups
TO7	Installationsscript Windows	Script, welches Windows Server als senden Host konfiguriert
TO8	Installationsscript Linux	Script, welches Linux Server als senden Host konfiguriert
TO9	Elasticsearch	Elasticsearch Installation
TO10	MongoDB	MongoDB Installation
TO11	Sendende Linux Server	Alle Lognachrichten sendenden Linux Server
TO12	Sendende Windows Server	Alle Lognachrichten sendenden Windows Server
TO13	Sendende Netzwerkkomponenten Server	Alle Lognachrichten sendenden Cisco Netzwerkkomponenten

Tabelle 58: Testobjekte



### 18.7.2 Testkategorien

Die nachfolgenden Testkategorien konnten von den Systemzielen und Anforderungen für dieses Projekt abgeleitet werden:

- Funktionelle Anwendertest
- Nicht funktionale Anwendertests
- Sicherheitstests

### 18.7.3 Testarten

Testart	Beschreibung
Black-Box-Test	Funktionsorientierte Tests welche durchgeführt werden, wenn keine Kenntnis über die innere Funktionsweise einer Komponente besteht.
White-Box-Test	Strukturorientierte Test, bei welchen mit Kenntnissen über die innere Funktionsweise einer Komponente getestet wird. z. B. Unit Tests.

Tabelle 59: Testarten

### 18.7.4 Testvoraussetzungen

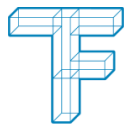
Um die in diesem Kapitel spezifizierten Test durchführen zu können, braucht es mindestens eine Testperson. Weiter muss das System vollständig realisiert sein. Um die Funktionalität beurteilen zu können, benötigt es Vorkenntnisse in der Funktionsweise des Endprodukts. Diese Vorkenntnisse werden im Rahmen der Realisierung dieses Projekts gewonnen.

### 18.7.5 Testvorgehen

Alle Tests werden nach der Realisierung des Projektes nacheinander durchgeführt. Falls ein Test fehlschlägt, muss ein entsprechendes Fehlerprotokoll (siehe 13.5.6 Fehlerprotokoll) ausgefüllt werden. Alle Tests werden in der umgesetzten Umgebung durchgeführt.

### 18.7.6 Testaccounts

Um alle Test durchführen zu können, wird ein Graylog Login benötigt. Wo nicht anders angegeben, wird das Domänenlogin der testenden Person verwendet.



### 18.7.7 Vorlage Testfälle

Die Tests werden anhand von Testfällen durchgeführt. Die Testfälle beschreiben genau, wie was zu testen ist. Mithilfe der nachfolgenden Vorlage werden die Testfälle spezifiziert und die Durchführung protokolliert:

Testfall ID	
Testobjekte	Welche Testobjekte werden benötigt?
Systemziele / Anforderungen	Welche Systemziele / Anforderungen werden durch diesen Test getestet?
Testbeschreibung	Was wird getestet?
Testvorgehen	Wie wird vorgegangen? Einzelne Schritte
Erwartet (Soll)	Welches Ergebnis wird erwartet?
Erwartet (Ist)	Wie ist das Ergebnis des Tests?
Kommentar / Screenshot	Kommentar / Screenshot zur Beschreibung des Tests

Tabelle 60: Vorlage Testfälle

### 18.7.8 Fehlerprotokoll

Falls ein Test nicht erfolgreich durchgeführt wird oder nicht das erwartete Resultat zurückliefert, muss ein Fehlerprotokoll ausgefüllt werden. Anhand dessen kann später nachvollzogen werden, was nicht funktioniert hat und wie der Fehler behoben werden kann. Falls der Fehler noch während diesem Projekt eliminiert wird, muss der identische Testfall wiederholt werden.

### 18.7.9 Vorlage Fehlerprotokoll

Folgende Vorlage ist für das Fehlerprotokoll zu verwenden:

Fehlerprotokoll	
Testfall ID	Testfall ID
Fehlerbeschreibung	Was hat nicht funktioniert? Bei welcher Aktion ist der Fehler aufgetreten? Möglichst genaue Beschreibung des aufgetretenen Fehler
Fehlerbehebung / Massnahmen	Wie wurde/wird der Fehler behoben? Wie kann der Fehler in Zukunft verhindert werden? Zukünftige Massnahmen?
Re-Testing	Wird der Test wiederholt? Wenn ja hat dieses funktioniert?

Tabelle 61: Vorlage Fehlerprotokoll

### 18.7.10 Testabnahme

Die Tests müssen von einer Testperson (Drittperson) begutachtet werden. Am Ende der Tests muss die Testabnahme von der Testperson und dem Projektleiter unterschrieben worden sein, um die Funktionalität und Korrektheit der Tests zu bestätigen.

Als Testperson ist gemäss dem Projektorganigramm Hetem Shaqiri vorgesehen.

## 18.7.11 Funktionelle Anwendertests

### 18.7.11.1 Testfall TF1 (Zugriff Graylog Web funktioniert)

Testfall TF1	
<b>Testobjekte</b>	TO2, TO3, TO4, TO9, TO10, F2
<b>Systemziele / Anforderungen</b>	S1, S2
<b>Testbeschreibung</b>	Graylog Webinterface kann angezeigt werden
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Öffnen eines Browsers</li> <li>2. Öffnen der URL <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>3. Login mit SHH Domänenaccount</li> </ol>
<b>Erwartet (Soll)</b>	Webinterface wird ohne Fehler angezeigt
<b>Erwartet (Ist)</b>	Ist auszufüllen...
<b>Kommentar / Screenshot</b>	Ist auszufüllen...

Tabelle 62: Testfall TF1 (Zugriff Graylog Web funktioniert)

### 18.7.11.2 Testfall TF2 (Installationsscript Windows Server 2008R2 funktioniert)

Testfall TF2	
<b>Testobjekte</b>	TO7
<b>Systemziele / Anforderungen</b>	S10, F7
<b>Testbeschreibung</b>	Das Script zur automatischen Konfiguration eines sendenden Windows Servers 2008R2 funktioniert.
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Starten einer VM mit der Grundinstallation von Windows Server 2008R2</li> <li>2. Ausführen des Installationsscript</li> <li>3. 3min warten</li> </ol>
<b>Erwartet (Soll)</b>	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
<b>Erwartet (Ist)</b>	Ist auszufüllen...
<b>Kommentar / Screenshot</b>	Ist auszufüllen...

Tabelle 63: Testfall TF2 (Installationsscript Windows Server 2008R2 funktioniert)

### 18.7.11.3 Testfall TF3 (Installationsscript Windows Server 2012 funktioniert)

Testfall TF3	
<b>Testobjekte</b>	TO7
<b>Systemziele / Anforderungen</b>	S10, F7
<b>Testbeschreibung</b>	Das Script zur automatischen Konfiguration eines sendenden Windows Servers 2012 funktioniert.
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Starten einer VM mit der Grundinstallation von Windows Server 2012</li> <li>2. Ausführen des Installationsscript</li> <li>3. 3min warten</li> </ol>
<b>Erwartet (Soll)</b>	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
<b>Erwartet (Ist)</b>	Ist auszufüllen...
<b>Kommentar / Screenshot</b>	Ist auszufüllen...

Tabelle 64: Testfall TF3 (Installationsscript Windows Server 2012 funktioniert)



#### 18.7.11.4 Testfall TF4 (Installationsscript Linux Server funktioniert)

Testfall TF4	
Testobjekte	TO8
Systemziele / Anforderungen	S10, F7
Testbeschreibung	Das Script zur automatischen Konfiguration eines sendenden Linux Servers funktioniert.
Testvorgehen	<ol style="list-style-type: none"><li>1. Starten einer VM mit der Grundinstallation von Debian Wheezy</li><li>2. Ausführen des Installationsscript</li><li>3. 3min warten</li></ol>
Erwartet (Soll)	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 65: Testfall TF4 (Installationsscript Linux Server funktioniert)

#### 18.7.11.5 Testfall TF5 (Backup funktioniert)

Testfall TF5	
Testobjekte	TO6
Systemziele / Anforderungen	S6
Testbeschreibung	Das Backup der wichtigsten Konfigurationsdateien von VMLOG1 funktioniert.
Testvorgehen	<ol style="list-style-type: none"><li>1. SSH Login auf VMLOG1</li><li>2. Restore vom gestrigen Tag vom File /etc/hosts mit dem Script in /bin/backup</li></ol>
Erwartet (Soll)	Datei wurde zurückgeholt
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 66: Testfall TF5 (Backup funktioniert)

#### 18.7.11.6 Testfall TF6 (Sendende Linux Server hinzugefügt)

Testfall TF6	
Testobjekte	TO11
Systemziele / Anforderungen	S8, F15
Testbeschreibung	Alle sendenden Linuxserver wurden konfiguriert und deren Lognachrichten sind in Graylog ersichtlich.
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Klick auf Sources in der Navigation</li><li>3. Setzen des Zeitlimits auf die letzten 30 Tage</li></ol>
Erwartet (Soll)	Alle Linux Server aus der Anforderung F15 sind hinzugefügt und in der Sources-Übersicht ersichtlich.
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 67: Testfall TF6 (Sendende Linux Server hinzugefügt)

#### 18.7.11.7 Testfall TF7 (Sendende Windows Server hinzugefügt)

Testfall TF7	
<b>Testobjekte</b>	TO12
<b>Systemziele / Anforderungen</b>	S8, F14
<b>Testbeschreibung</b>	Alle sendenden Windowsserver wurden konfiguriert und deren Lognachrichten sind in Graylog ersichtlich.
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>2. Klick auf Sources in der Navigation</li> <li>3. Setzen des Zeitlimit auf die letzten 30 Tage</li> </ol>
<b>Erwartet (Soll)</b>	Alle Windows Server aus der Anforderung F14 sind hinzugefügt und in der Sources-Übersicht ersichtlich.
<b>Erwartet (Ist)</b>	Ist auszufüllen...
<b>Kommentar / Screenshot</b>	Ist auszufüllen...

Tabelle 68: Testfall TF7 (Sendende Windows Server hinzugefügt)

#### 18.7.11.8 Testfall TF8 (Sendende Netzwerkkomponenten hinzugefügt)

Testfall TF 8	
<b>Testobjekte</b>	TO13
<b>Systemziele / Anforderungen</b>	S8, F16
<b>Testbeschreibung</b>	Alle sendenden Netzwerkkomponenten wurden konfiguriert und deren Lognachrichten sind in Graylog ersichtlich.
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>2. Klick auf Sources in der Navigation</li> <li>3. Setzen des Zeitlimit auf die letzten 30 Tage</li> </ol>
<b>Erwartet (Soll)</b>	Alle Netzwerkkomponenten aus der Anforderung F16 sind hinzugefügt und in der Sources-Übersicht ersichtlich.
<b>Erwartet (Ist)</b>	Ist auszufüllen...
<b>Kommentar / Screenshot</b>	Ist auszufüllen...

Tabelle 69: Testfall TF8 (Sendende Netzwerkkomponenten hinzugefügt)

#### 18.7.11.9 Testfall TF9 (Monitoring VMLOG1 ersichtlich)

Testfall TF9	
<b>Testobjekte</b>	TO5
<b>Systemziele / Anforderungen</b>	S7, F6
<b>Testbeschreibung</b>	Das Monitoring ist eingerichtet und im Icinga ersichtlich
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Öffnen von <a href="https://vmmon1.lwb.ch/icinga-web/">https://vmmon1.lwb.ch/icinga-web/</a></li> <li>2. Suchen nach VMLOG1</li> </ol>
<b>Erwartet (Soll)</b>	Der Server VMLOG1 wird gemäss Monitoring-Konzept (Seite 70) überwacht.
<b>Erwartet (Ist)</b>	Ist auszufüllen...
<b>Kommentar / Screenshot</b>	Ist auszufüllen...

Tabelle 70: Testfall TF9 (Monitoring VMLOG1 ersichtlich)





18.7.11.10 Testfall TF10 (Graylog Streams eingerichtet)

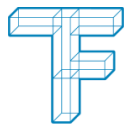
Testfall TF10	
Testobjekte	TO2, TO3, TO4, TO9, TO10
Systemziele / Anforderungen	S1, S2, S9, F2, F3, F10, F11, F12
Testbeschreibung	Die Graylog Streams wurden inklusive der Alarmierung eingerichtet.
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Klick auf Streams in der Navigation</li></ol>
Erwartet (Soll)	<p>Die nachfolgenden Streams sind in der Übersicht vorhanden:</p> <ul style="list-style-type: none"><li>• Windows</li><li>• Linux</li><li>• Cisco</li><li>• Ungültige SSH Logins</li><li>• Windows Server Crash Shutdown</li></ul> <p>Weiter sind die nachfolgenden Alarme ersichtlich.</p> <ul style="list-style-type: none"><li>• DFSR Fehler</li><li>• Ungültige SSH Logins</li><li>• Windows Server Crash Shutdown</li></ul>
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 71: Testfall TF10 (Graylog Streams eingerichtet)

18.7.11.11 Testfall TF11 (Graylog Übersichtsdashboard eingerichtet)

Testfall TF11	
Testobjekte	TO2, TO3, TO4, TO9, TO10
Systemziele / Anforderungen	S1, S2, F2, F13
Testbeschreibung	Das Graylog Übersichtsdashboard ist eingerichtet
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Klick auf „Dashboards“ in der Navigation</li></ol>
Erwartet (Soll)	Es ist ein Dashboard mit den wichtigsten Kennzahlen verfügbar.
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 72: Testfall TF11 (Graylog Übersichtsdashboard eingerichtet)



## 18.7.12 Nicht funktionale Anwendertests

### 18.7.12.1 Testfall TF12 (Schneller Zugriff auf Webinterface)

Testfall TF12	
Testobjekte	TO2, TO3, TO4, TO9, TO10
Systemziele / Anforderungen	NF2
Testbeschreibung	Dieser Test stellt sicher, dass der Zugriff auf das Graylog Webinterface schnell möglich ist
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a> im Google Chrome</li><li>2. Öffnen der Developer Tools (F12)</li><li>3. Klick auf Network in den Developer Tools</li><li>4. Suche nach allen Logs in den letzten 5min</li></ol>
Erwartet (Soll)	Die Ladezeit beträgt weniger als 5s
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 73: Testfall TF12 (Schneller Zugriff auf Webinterface)

## 18.7.13 Sicherheitstest

### 18.7.13.1 Testfall TF13 (Anmeldung für Mitglieder G\_MA-INF)

Testfall TF13	
Testobjekte	TO2, TO3, TO4, TO9, TO10
Systemziele / Anforderungen	F8, F9
Testbeschreibung	Dieser Test stellt sicher, dass sich ein Benutzer, mit Mitgliedschaft in der Gruppe G_MA-INF, am Graylog Webinterface anmelden kann.
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Login mit dem Benutzer SHH</li></ol>
Erwartet (Soll)	Login erfolgreich
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 74: Testfall TF13 (Anmeldung für Mitglieder G\_MA-INF)

### 18.7.13.2 Testfall TF14 (Anmeldung für Nicht-Mitglieder G\_MA-INF)

Testfall TF14	
Testobjekte	TO2, TO3, TO4, TO9, TO10
Systemziele / Anforderungen	F8, F9
Testbeschreibung	Dieser Test stellt sicher, dass sich ein Benutzer, welcher nicht Mitglied der Gruppe G_MA-INF ist, sich nicht am Graylog Webinterface anmelden kann.
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Login mit dem Benutzer TEST-V</li></ol>
Erwartet (Soll)	Login schlägt mit Fehlermeldung fehl.
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 75: Testfall TF14 (Anmeldung für Nicht-Mitglieder G\_MA-INF)



#### 18.7.13.3 Testfall TF15 (Webinterface ist verschlüsselt)

Testfall TF15	
Testobjekte	TO3, TO4
Systemziele / Anforderungen	S2, F4
Testbeschreibung	Dieser Test stellt sicher, dass der Zugriff auf das Webinterface verschlüsselt erfolgt.
Testvorgehen	1. Öffnen von <a href="http://log.lwb.ch">http://log.lwb.ch</a>
Erwartet (Soll)	Der Benutzer wird automatisch von <a href="http://log.lwb.ch">http://log.lwb.ch</a> nach <a href="https://log.lwb.ch">https://log.lwb.ch</a> weitergeleitet. Es erscheint keinerlei Fehler, welcher die Verschlüsselung betrifft.
Erwartet (Ist)	Ist auszufüllen...
Kommentar / Screenshot	Ist auszufüllen...

Tabelle 76: Testfall TF15 (Anmeldung für Nicht-Mitglieder G\_MA-INF)

## 19. Realisierung

Die nachfolgenden Unterkapitel zeigen die Realisierung des Projekts. Es wird lediglich auf die Einstellungen eingegangen, welche nicht den Standardeinstellungen entsprechen.

### 19.1 Grundinstallation VMLOG1

#### 19.1.1 Verbindung zum vCenter

In einem ersten Schritt muss mithilfe des vSphere Clients auf den vCenter Server zugegriffen. Dazu muss das nachfolgende Login benutzt werden:

Attribut	Wert
IP-Adresse	86.118.120.180
Benutzername	LWB\Administrator
Passwort	siehe Keepass

Tabelle 77: vCenter Login

#### 19.1.2 Erstellen der VM

In einem nächsten Schritt wird die benötigte VM erstellt. Da auf dem esx1 zurzeit weniger Last ist, wird sie auf dem diesem Server erstellt. Später kann sie jedoch auch problemlos auf den esx2 Server verschoben werden. Zum Erstellen sind die nachfolgenden Schritte nötig:

- **Auswählen von „esx1“** in der Navigation auf der linken Seite
- **Klick** auf das nachfolgend markierte Symbol

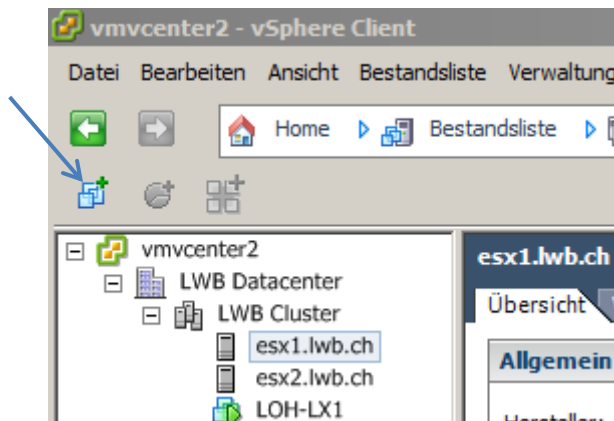


Abbildung 7: Symbol VM erstellen

- Konfiguration: Typisch
- Als Namen **VMLOG1** eingeben und bestätigen mit „Weiter“
- Als Speicherort **„R5-10k-SANDisk1“** (SAN) wählen
- Das Gastbetriebssystem auf **Linux - „Debian GNU/Linux 6 (64 bit)“** festlegen (Debian 7 ist als Auswahl nicht verfügbar, funktioniert jedoch problemlos mit der Debian 6)
- Die Netzwerkkarte wird in das **Service** Netzwerk gehängt
- Die Festplatte wird auf **20 GB - Thick-Provision Lazy Zeroed** festgelegt
- Vor dem Klick auf „Fertigstellen“ bzw. „Beenden“ wird noch das Häkchen **„Einstellungen der virtuellen Maschine vor der Fertigstellung bearbeiten“** angekreuzt

- Ändern des **Arbeitsspeichers auf 4 GB**
- Ändern der CPU Einstellung „**Anzahl Cores pro Socket**“ auf **2**
- Entfernen des Diskettenlaufwerk
- Hinzufügen einer zusätzlichen, neuen Festplatte
  - Die Konfiguration wird auf **75 GB - Thick-Provision Lazy Zeroed** festgelegt
  - Alle anderen Einstellungen können auf Standard belassen werden
- Unter dem CD Laufwerk wird das Debian Installations-ISO eingehängt (**[R5-10k-SANDisk1] ! ISOs/debian-7.1.0-amd64-netinst.iso**). Weiter muss das Häkchen „**Beim Einschalten verbinden**“ gesetzt sein.
- Am Ende soll das Ergebnis folgendermassen aussehen:

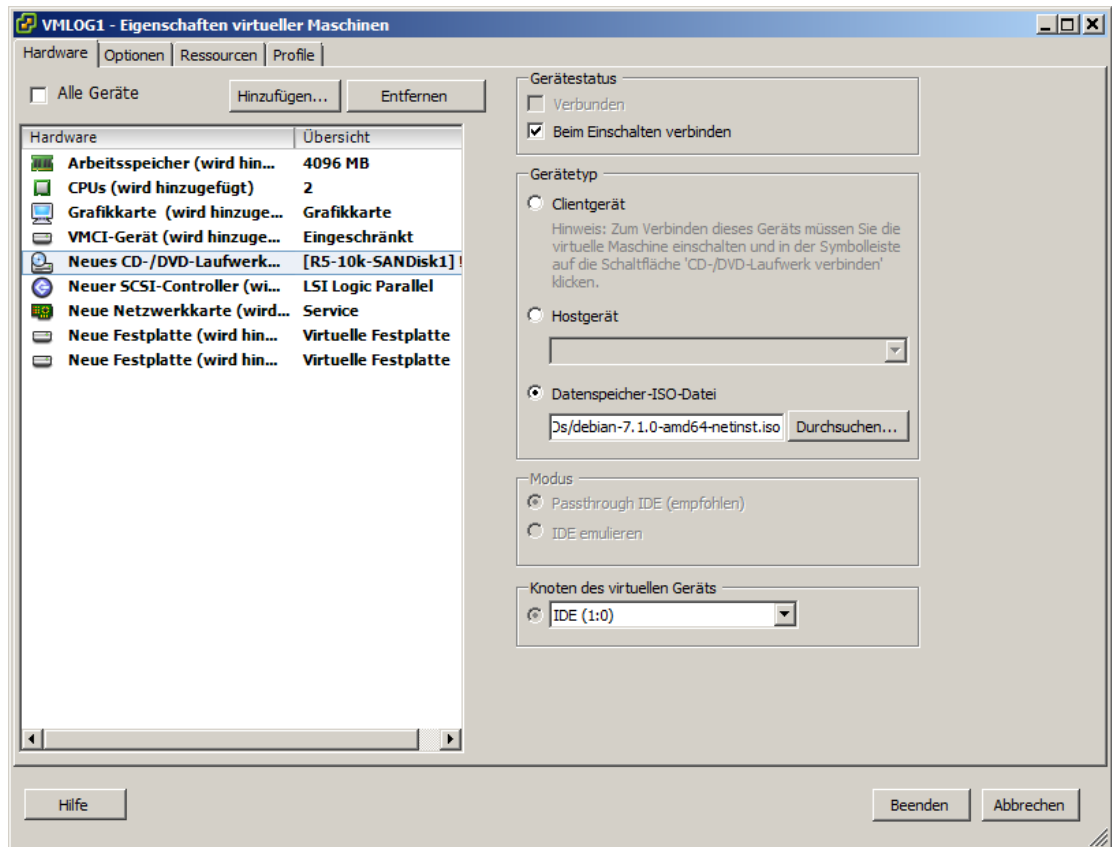


Abbildung 8: Soll - VM erstellen

- Klick auf **Beenden**

### 19.1.3 Debian Installation

Als nächster Schritt muss das Betriebssystem installiert werden. Dazu sind die nachfolgenden Schritte notwendig:

- Start der eben erstellten VM VMLOG1
- Öffnen der VM Konsole
- Wählen von **Install** im Debian Installer
  - Festlegen der Regionseinstellungen
  - Als Sprache wird „**English**“ gewählt
  - Die „Location“ Einstellung wird auf „**Switzerland**“ gesetzt

- „Default locale“ : „**en\_US.UTF-8**“
- Das Tastaturlayout wird auf Swiss German festgelegt
- Anschliessend kann der Hostname auf „**VMLOG1**“ gesetzt werden
- Der Domänenname wird auf **lwb.ch** gesetzt
- In einem nächsten Schritt wird das Root-Passwort gesetzt. Dieses entspricht dem TF Bern Passwort für Linux Server (siehe Keepass)
- In einem nächsten Schritt muss ein zweiter Benutzer erstellt werden. Da dieser Benutzer später gelöscht wird, sind die Einstellungen egal
- Formatieren der Festplatte
  - „**Guided - use entire disk**“ auswählen
  - Auswählen der **kleineren Festplatte** (entspricht der 1. Festplatte)
  - Partitioning scheme: **All files in one partition**
  - **Finish**
  - Write changes to disk: **yes**
- Setzender Debian Mirror
  - Debian archive mirror country: **Switzerland**
  - Archive Mirror: **mirror.switch.ch**
  - HTTP Proxy kann leer gelassen werden
- Participate in the package usage survey: **No**
- Bei der Softwareauswahl wird die folgende Auswahl getroffen, um ein schlankes System zu erhalten, auf welches über SSH zugegriffen werden kann:

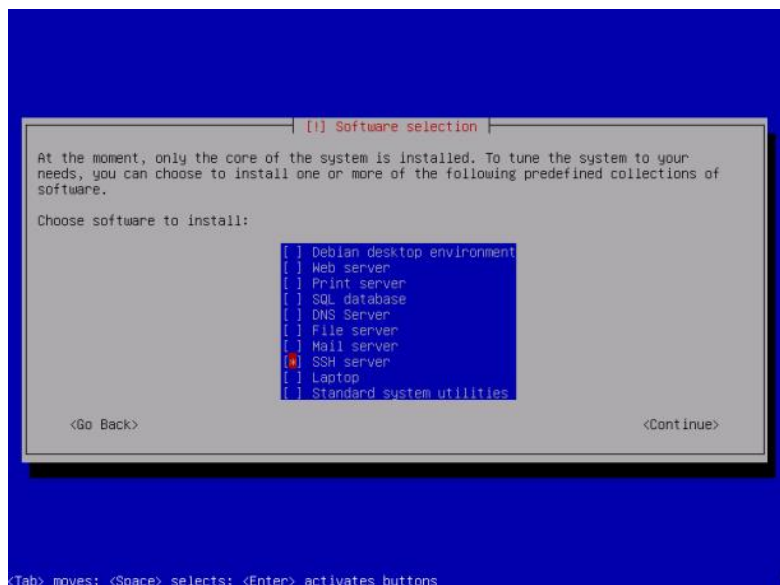


Abbildung 9: Softwareauswahl - Debian Installer

- Install the GRUB boot loader to the master boot record?: **Yes**
- Anschliessend muss das System neugestartet werden, um die Installation abzuschliessen

Wie angekündigt wird der erstellte User gelöscht, da er nicht benutzt wird:

```
root@VMLOG1:~# userdel user
root@VMLOG1:~# rm -rf /home/user
```

#### 19.1.4 Netzwerkkonfiguration

Um die Netzwerkkonfiguration gemäss dem Konzept einzurichten, ist es notwendig die folgenden Schritte zu unternehmen:

```
root@VMLOG1:~# nano /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 86.118.120.30
    netmask 255.255.255.0
    network 86.118.120.0
    broadcast 86.118.120.255
    gateway 86.118.120.1
    # dns-* options are implemented by the resolvconf package, if
    installed
    dns-nameservers 86.118.120.170 86.118.120.171
    dns-search lwb.ch
```

Leider funktioniert der blosse Neustart des Netzwerkes über „/etc/init.d/networking restart“ bei aktuellen Debian und Ubuntu Versionen nicht mehr einwandfrei. Aus diesem Grund ist der Server vollständig neu zu starten:

```
init 6
```

#### 19.1.5 Updaten des Systems

Grundsätzlich sollte ein System nach einer Installation mit dem Debian Installer auf dem aktuellen Stand sein. Da dies aber nicht immer wie gewünscht funktioniert, wird dies mit den nachfolgenden Befehlen überprüft und allenfalls erledigt.

```
root@VMLOG1:~# apt-get update
root@VMLOG1:~# apt-get upgrade
```

### 19.1.6 Installation VMWare Tools

Da installierte VMWare Tools, die Performance einer VM erheblich steigern können, werden diese in einem nächsten Schritt installiert.

Es bestehen einige Abhängigkeiten, welche vorab installiert werden müssen:

```
root@VMLOG1:~# apt-get install build-essential
root@VMLOG1:~# apt-get install linux-headers-$(uname -r)
```

Anschliessend können die Tools von einer ISO Datei installiert werden. Diese kann über den vSphere Client eingelegt werden: Rechtsklick auf die VM VMLOG1 -> Gast -> „VMWare Tools installieren“.

Nun kann der Inhalt der CD auf die VM kopiert und entpackt werden:

```
root@VMLOG1:~# mount /dev/cdrom /mnt
root@VMLOG1:~# cp /mnt/VMwareTools-*.tar.gz /usr/src
root@VMLOG1:/usr/src# cd /usr/src
root@VMLOG1:/usr/src# tar -xzf VMwareTools-*.tar.gz
```

Nun kann die CD wieder getrennt werden:

```
root@VMLOG1:/usr/src# umount /mnt
```

Mit dem nachfolgenden Befehl wird die Installation gestartet. Sämtliche Einstellungen können auf dem Standard belassen werden und müssen nur mit „Enter“ bestätigt werden:

```
root@VMLOG1:/usr/src# /usr/src/vmware-tools-distrib/vmware-install.pl
```

Damit die VMWare Tools funktionieren, muss der Server neugestartet werden:

```
root@VMLOG1:/usr/src# init 6
```

Nach erfolgreicher Installation ist der Status der VMWare Tools im vSphere Client ersichtlich:

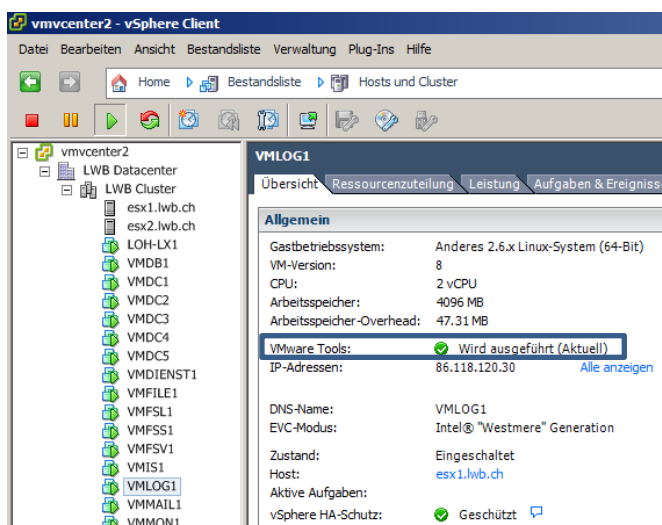


Abbildung 10: VMware Tools Status




### 19.1.7 Festplatte mounten

In einem nächsten Schritt wird die sekundäre Festplatte formatiert und eingehängt. Dazu wird zuerst ein nützliches Tool installiert, mit welchem sich die Eigenschaften aller Geräte anzeigen lassen:

```
root@VMLOG1:~# apt-get install lshw
```

Mit Hilfe des eben installierten Tools lshw ist es möglich den richtigen Devicepfad auszulesen:

```
root@VMLOG1:~# lshw -class disk
...
*-disk:1
   description: SCSI Disk
   physical id: 0.1.0
   bus info: scsi@0:0.1.0
   logical name: /dev/sdb
   size: 75GiB (80GB)
   configuration: sectorsize=512
```



Anschliessend kann die Festplatte partitioniert werden:

```
root@VMLOG1:~# fdisk /dev/sdb
...
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-157286399, default 2048): 2048
Last sector, +sectors or +size{K,M,G} (2048-157286399, default
157286399): 157286399
```

Nun kann die Festplatte formatiert werden. Als Filesystem wird ext3 gewählt.

```
root@VMLOG1:~# mkfs.ext3 /dev/sdb1
```

Als nächster Schritt muss das Mount-Verzeichnis erstellt werden, in diesem Fall ist dies „/data“.

```
root@VMLOG1:~# mkdir /data
```

In einem letzten Schritt muss die Datei angepasst werden, in welche die beim Systemstart zu mountenden Festplatten eingetragen sind. Wichtig ist dabei, dass diese Datei absolut fehlerfrei ist, da es ansonsten passieren kann, dass das System nicht mehr bootet.

```
root@VMLOG1:~# nano /etc/fstab

...
/dev/sdb1      /data          ext3           defaults      1             2
```



Damit die Änderungen übernommen werden, muss das System mit dem nachfolgenden Befehl neu gestartet werden.

```
root@VMLOG1:~# init 6
```

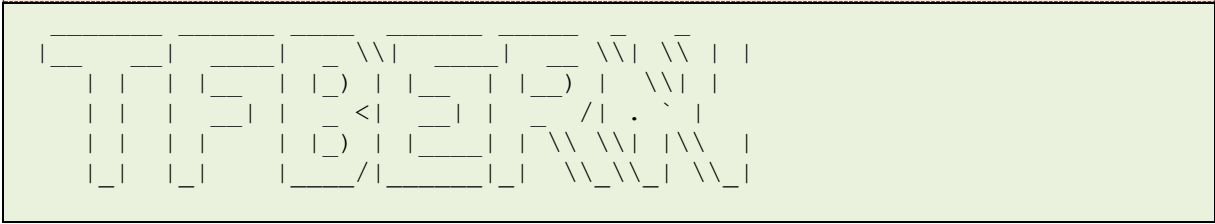
Die Änderungen können überprüft werden, indem der Ordnerinhalt des „data“ Verzeichnisses angezeigt wird. Nach erfolgreichem Mounten der sekundären Disk ist ein „lost+found“ Ordner ersichtlich:

```
root@VMLOG1:~# ls /data  
lost+found
```

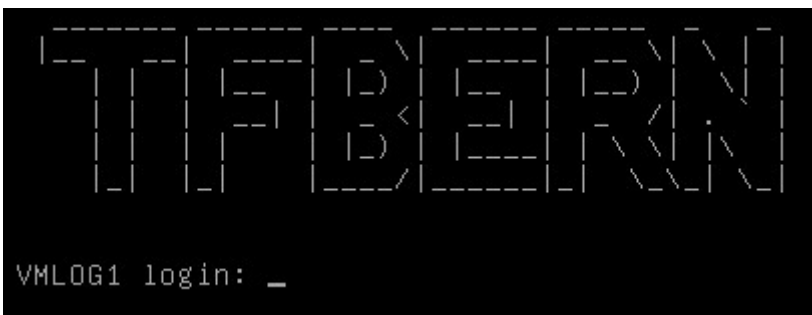
### 19.1.8 Logonscreen

Um im Logonscreen einen TF Bern Schriftzug anzuzeigen, ist der nachfolgende Schritt notwendig:

```
root@VMLOG1:~# nano /etc/issue
```



Da ein Backslash in der „etc/issue“ Datei als Escape Character wirkt, sind alle Backslashes doppelt vorhanden. Im Willkommensbildschirm funktioniert die Anzeige anschliessend wie gewünscht.



**Tabelle 78: Logonscreen (Soll)**

### 19.1.9 Willkommensscreen

Der Willkommensscreen nach dem Anmelden eines Benutzers soll ebenfalls einen TF Bern Schriftzug tragen. Dies wird mit dem nachfolgenden Schritt erreicht:

```
root@VMLOG1:~# nano /etc/motd
```



TFB BERN

Weiter soll nach der Anmeldung eine Übersicht über die aktuelle Auslastung erscheinen. Dazu wird das Tool „Archey“ verwendet. Es wird mit den nachfolgenden Schritten installiert:

```
root@VMLOG1:~# apt-get install lsb-release scrot
root@VMLOG1:~# wget http://github.com/downloads/djmelik/archey/archey-
0.2.8.deb --no-check-certificate
root@VMLOG1:~# dpkg -i archey-0.2.8.deb
root@VMLOG1:~# rm archey-0.2.8.deb
```

Damit auch der Archey Screen bei jedem erfolgreichen Login automatisch erscheint, ist es nötig eine Anpassung an „/etc/bash.bashrc“ vorzunehmen.

```
root@VMLOG1:~# nano /etc/bash.bashrc
```

```
...
archey
```

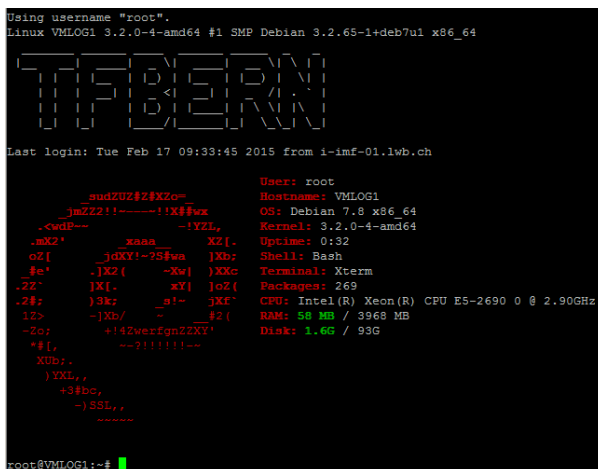


Tabelle 79: Willkommensbildschirm (Soll)

### 19.1.10 DNS Einträge

Damit der Server VMLOG1 einfacher angesprochen werden kann, wurden die nachfolgenden Einträge auf einem DNS Server eines „lwb.ch“ Domaincontrollers erstellt.

Name/IP	Typ	Name/IP	Zone
VMLOG1	A	86.118.120.30	lwb.ch.
log	CNAME	VMLOG1.lwb.ch.	lwb.ch.
86.118.120.30	PTR	VMLOG1.lwb.ch.	120.118.86.in-addr.arpa.

Tabelle 80: DNS Einträge Logserver



## 19.2 Installation Java

In einem nächsten Schritt wird Java installiert. Da in der Vergangenheit schlechte Erfahrungen mit dem OpenJDK gemacht wurden, wird Oracle Java 8 verwendet.

Zuerst müssen die Paketquellen angepasst werden. Die hier verwendete Paketquelle ist eigentlich für Ubuntu und nicht für Debian. Da das später installierte Paket aber nur den offiziellen Oracle Java Installer herunterlädt, ist dies kein Problem.

```
root@VMLOG1:~# nano /etc/apt/sources.list.d/java.list
deb http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main
deb-src http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main

root@VMLOG1:~# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --
recv-keys EEA14886
```

Nun können die Paketlisten aktualisiert und Java installiert werden:

```
root@VMLOG1:~# apt-get update
root@VMLOG1:~# apt-get install oracle-java8-installer
```

Mit dem nachfolgenden Befehl kann die Installation überprüft werden:

```
root@VMLOG1:~# javac -version
javac 1.8.0_31
```

## 19.3 Installation MongoDB

Nun wird MongoDB installiert. Da die MongoDB Version in den offiziellen Debian Paketquellen stark veraltet ist, wird auf die aktuelle Version des MongoDB Repos zurückgegriffen. Aus diesem Grund muss erneut eine Paketquelle hinzugefügt werden:

```
root@VMLOG1:~# nano /etc/apt/sources.list.d/mongodb.list
deb http://downloads-distro.mongodb.org/repo/debian-sysvinit dist 10gen

root@VMLOG1:~# apt-key adv --keyserver keyserver.ubuntu.com --recv
7F0CEB10
```

Nun können die Paketlisten aktualisiert und MongoDB installiert werden:

```
root@VMLOG1:~# apt-get update
root@VMLOG1:~# apt-get install mongodb-org
```

Da die Konfiguration noch nicht ordnungsgemäss ist, wird der MongoDB Service vorerst gestoppt.

```
root@VMLOG1:~# /etc/init.d/mongod stop
```

In einem nächsten Schritt, wird das Datenverzeichnis der MongoDB auf „/data/mongodb“ angepasst dazu sind die nachfolgenden Schritte notwendig:



```
root@VMLOG1:~# mv /var/lib/mongodb /data
root@VMLOG1:~# ln -s /data/mongodb /var/lib/
root@VMLOG1:~# nano /etc/mongod.conf

dbpath=/data/mongodb
```

Nun kann der MongoDB Service wieder gestartet werden.

```
root@VMLOG1:~# /etc/init.d/mongod start
```

Die ordnungsgemässe Funktionsweise kann mit den nachfolgenden Befehlen überprüft werden.

```
root@VMLOG1:~# mongo
> show dbs
admin (empty)
local 0.078GB
> quit()
```

## 19.4 Installation Elasticsearch

Zur Installation von Elasticsearch müssen erneut die Paketquellen angepasst werden. Dazu sind die nachfolgenden Schritte notwendig:

```
root@VMLOG1:~# nano /etc/apt/sources.list.d/elasticsearch.list
deb http://packages.elasticsearch.org/elasticsearch/1.4/debian stable
main

root@VMLOG1:~# wget https://packages.elasticsearch.org/GPG-KEY-
elasticsearch --no-check-certificate
root@VMLOG1:~# apt-key add GPG-KEY-elasticsearch
root@VMLOG1:~# rm GPG-KEY-elasticsearch
```

Nun können die Paketlisten aktualisiert und Elasticsearch installiert werden:

```
root@VMLOG1:~# apt-get update
root@VMLOG1:~# apt-get install elasticsearch
```

Damit Elasticsearch automatisch gestartet wird, muss die Init-Konfiguration angepasst werden.

```
update-rc.d elasticsearch defaults 95 10
```

Nun muss die Elasticsearch Konfiguration angepasst werden:

```
root@VMLOG1:~# nano /etc/elasticsearch/elasticsearch.yml
...
cluster.name: graylog2
...
network.bind_host: 127.0.0.1
```



```
...  
path.data: /data/elasticsearch/data  
...  
script.disable_dynamic: true  
...  
network.publish_host: 127.0.0.1  
...  
network.host: 127.0.0.1
```

Da das Datenverzeichnis geändert wurde, muss dieses von Hand erstellt und berechtigt werden:

```
root@VMLOG1:~# mkdir -p /data/elasticsearch/data  
root@VMLOG1:~# chown -R elasticsearch:elasticsearch /data/elasticsearch/  
root@VMLOG1:~# chmod -R 770 /data/elasticsearch/  
root@VMLOG1:~# ln -s /data/elasticsearch/data/ /var/lib/elasticsearch/
```

Da Elasticsearch zeitweilen etwas RAM-Hungrig ist, wird die maximale Heap-Size auf 2 GB beschränkt:

```
root@VMLOG1:~# nano /etc/init.d/elasticsearch  
ES_HEAP_SIZE=2g
```

Nun kann Elasticsearch gestartet werden:

```
root@VMLOG1:~# /etc/init.d/elasticsearch start
```

Mit dem nachfolgenden Befehl kann getestet werden, ob die Installation und Konfiguration von Elasticsearch erfolgreich war.

```
root@VMLOG1:~# curl -XGET  
'http://localhost:9200/_cluster/health?pretty=true'  
{  
  "cluster_name" : "graylog2",  
  "status" : "green",  
  ...  
}
```

## 19.5 Graylog Server Installation

Zur Graylog Server Installation sind die nachfolgenden Schritte notwendig:

```
root@VMLOG1:~# wget https://packages.graylog2.org/repo/packages/graylog2-  
0.92-repository-debian7_latest.deb  
root@VMLOG1:~# dpkg -i graylog2-0.92-repository-debian7_latest.deb  
root@VMLOG1:~# apt-get install apt-transport-https  
root@VMLOG1:~# apt-get update  
root@VMLOG1:~# apt-get install graylog2-server  
root@VMLOG1:~# rm graylog2-0.92-repository-debian7_latest.deb
```



Um die von Graylog verwendete Secret Keys zu generieren, wird pwgen benutzt. Dieses Tool muss zuerst installiert werden:

```
root@VMLOG1:~# apt-get install pwgen
```

Nun muss das Graylog admin Passwort und ein Passwort Secret gesetzt werden:

```
root@VMLOG1:~# SECRET=$(pwgen -s 96 1)
root@VMLOG1:~# sed -i -e 's/password_secret =.*/password_secret =
'$SECRET'/' /etc/graylog2.conf
root@VMLOG1:~# PASSWORD=$(echo -n geheimesPasswort | shasum -a 256 | awk
'{print $1}')
root@VMLOG1:~# sudo -E sed -i -e 's/root_password_sha2
=.*root_password_sha2 = '$PASSWORD'/' /etc/graylog2.conf
```

Nun müssen einige grundlegende Konfigurationen vorgenommen werden:

```
root@VMLOG1:~# nano /etc/graylog2.conf
...
rest_transport_uri = http://127.0.0.1:12900/
...
elasticsearch_shards = 1
...
elasticsearch_discovery_zen_ping_multicast_enabled = false
elasticsearch_discovery_zen_ping_unicast_hosts = 127.0.0.1:9300
...
elasticsearch_max_docs_per_index = 2000000
...
elasticsearch_max_number_of_indices = 30
...
transport_email_enabled = true
transport_email_hostname = 127.0.0.1
transport_email_port = 25
transport_email_use_auth = false
transport_email_use_tls = false
transport_email_use_ssl = false
...
transport_email_from_email = log@lwb.ch
...
```

Nun kann Graylog Server im Debug Modus gestartet werden um die Konfiguration zu überprüfen:

```
root@VMLOG1:~# java -jar /usr/share/graylog2-server/graylog2-server.jar -
-debug
...
2015-02-17 12:00:08,293 INFO : org.graylog2.Main - Graylog2 Server up and
running.
...
```

## 19.6 Graylog Web

Da für weitere Konfigurationen des Graylog Servers das Webinterface Graylog Web benötigt wird, muss dieses vor Abschluss aller Graylog Konfiguration installiert werden. Dazu ist der nachfolgende Befehl notwendig:

```
root@VMLOG1:~# apt-get install graylog2-web
```

Auch für Graylog Web wird ein Secret Key benötigt, welcher mit den nachfolgenden Befehlen gesetzt wird:

```
root@VMLOG1:~# SECRET=$(pwgen -s 96 1)
root@VMLOG1:~# sed -i -e
's/application\.secret=""/application\.secret="'$SECRET'"/'
/etc/graylog2/web/graylog2-web-interface.conf
```

Anschliessend muss noch die URL zum Graylog Server angepasst werden:

```
root@VMLOG1:~# nano /etc/graylog2/web/graylog2-web-interface.conf
graylog2-server.uris=http://127.0.0.1:12900/
```

Dies war schon die gesamte benötigte Konfiguration des Webinterface. Es muss lediglich noch gestartet werden:

```
root@VMLOG1:~# /etc/init.d/graylog2-web start
```

Nun kann das Webinterface unter <http://log.lwb.ch:9000/> erreicht werden. Achtung: Der Zugriff auf diese URL ist unverschlüsselt und sollte nur solange verwendet werden, bis der nginx Reverse Proxy konfiguriert ist.

## 19.7 Graylog Input Konfiguration

Der benötigte Graylog Input wird über das Webinterface hinzugefügt. Folgende Schritte sind dazu notwendig:

- Login im Graylog Webinterface
- Öffnen der **Inputeinstellungsseite** (System -> Inputs)
- Betätigen des Buttons „**Launch new Input**“ mit vorheriger Einstellung von „**GELF UDP**“
- Setzen des Häkchens „**Global Input**“
- Setzen des Titels auf „**From Logstash**“
- Alle anderen Einstellungen können auf dem Standardwert belassen werden
- Klick auf „**Launch**“





System / Inputs

## Inputs in Cluster

Graylog2 nodes accept data via inputs. Launch or terminate as many inputs as you want here.

AMQP Input Launch new input

### Running global inputs

From Logstash (GELF UDP) 1 running

Started by Administrator a minute ago

Pause

Terminate

Action

Network ID: 0B-0B (total: 0B-0B) Show details

```
override_source:  
recv_buffer_size: 1048576  
bind_address: 0.0.0.0  
port: 12201
```

Abbildung 11: Erwartetes Ergebnis

## 19.8 Graylog LDAP Konfiguration

Um Graylog mit dem AD koppeln zu können, muss ein Benutzer mit Leserechten im AD vorhanden sein. Für diesen Zweck wurde ein Benutzer im AD der Domäne „lwb.ch“ mit folgenden Werten erstellt.

Attribut	Wert
Nachname	GRAYLOG
Voller Name	GRAYLOG
Login Name	GRAYLOG
Passwort	siehe Keepass
Passwort beim nächsten Login ändern	Nein
Passwort läuft nie ab	Ja
Benutzer kann Passwort nicht ändern	Ja
Account deaktiviert	Nein
OU	OU=USER,OU=SERVICE,OU=LO,OU=LWB,DC=lwb,DC=ch

Die benötigte Graylog LDAP Konfiguration wird über das Webinterface vorgenommen. Folgende Schritte sind dazu notwendig:

- Login im Graylog Webinterface
- Öffnen der **LDAP-Einstellungsseite** (System -> Users -> Configure LDAP)
- Vornehmen der Serverkonfiguration gemäss dem untenstehenden Bild:

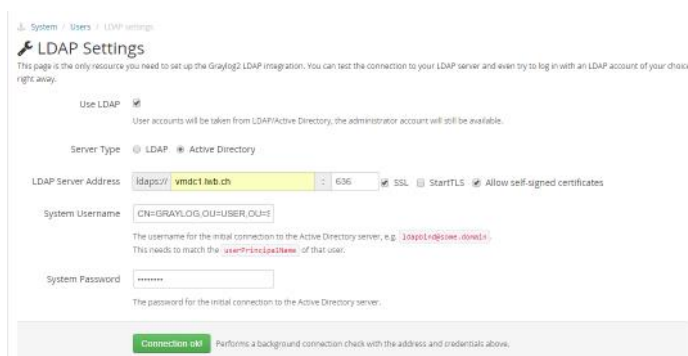


Abbildung 12: Graylog LDAP: Serverkonfiguration

- Vornehmen der erweiterten Konfiguration gemäss untenstehendem Bild:

Search Base DN

The base tree to limit the Active Directory search query to, e.g. `cn=users,dc=example,dc=com`

User Search Pattern

For example `(&(objectClass=user)(sAMAccountName={0}))`. The string `{0}` will be replaced by the entered username.

Display Name attribute

If you are unsure which attribute to use, try to load a test user using the form below.  
Which Active Directory attribute to use for the full name of the user in Graylog2, e.g. `displayName`.

Default permission group

This determines the default set of permissions a user will be assigned.

**Abbildung 13: Graylog LDAP: Erweiterte Konfiguration**

**Hinweis:** Das User Search Pattern beträgt

„(&(objectClass=user)(sAMAccountName={0})(memberof=CN=G\_MA-INF,OU=G\_GROUP,OU=GROUP,OU=LWB,DC=lwb,DC=ch))“ und schränkt die Anmeldung so ein, dass nur noch Mitglieder der Gruppe „G\_MA-INF“ zur Anmeldung berechtigt sind.

- Speichern

## 19.9 Logstash Installation

Da es nahezu unmöglich ist, weitere Graylog Konfigurationen ohne empfangene Logs zu erfassen, wurde als nächster Schritt Logstash installiert.

Als erster Schritt ist es notwendig die Paketlisten anzupassen. Dies wird mit der nachfolgenden Anpassung erledigt:

```
root@VMLOG1:~# nano /etc/apt/sources.list.d/logstash.list
deb http://packages.elasticsearch.org/logstash/1.4/debian stable main
```

Nun können die Paketlisten aktualisiert und Logstash installiert werden:

```
root@VMLOG1:~# apt-get update
root@VMLOG1:~# apt-get install logstash
```

Zur Authentifizierung an Logstash, über das Lumberjack Protokoll, werden Zertifikate verwendet. Die notwendigen Verzeichnisse und Zertifikate müssen manuell erstellt werden. Es wird ein Zertifikat verwendet, welches 10 Jahre gültig ist. Zur Erstellung sind die nachfolgenden Schritte notwendig:

```
root@VMLOG1:~# mkdir -p /etc/pki/tls/certs
root@VMLOG1:~# mkdir /etc/pki/tls/private
root@VMLOG1:~# cd /etc/pki/tls/
root@VMLOG1:/etc/pki/tls# openssl req -x509 -batch -nodes -days 3652 -
newkey rsa:2048 -keyout private/logstash-forwarder.key -out
certs/logstash-forwarder.crt
```



Damit Logstash beim Serverneustart automatisch gestartet wird, muss mit dem nachfolgenden Befehl die Init Konfiguration angepasst werden:

```
update-rc.d logstash defaults
```

Logstash liefert standardmässig ein eigenes Webinterface mit. Da dieses nicht verwendet wird, wird es mit den nachfolgenden Schritten deaktiviert:

```
root@VMLOG1:~# nano /etc/init/logstash-web.conf
```

```
...  
start on never  
...
```

```
root@VMLOG1:~# update-rc.d -f logstash-web remove
```

## 19.10 Logstash Linux Input Konfiguration

Zu Erstellung des Logstash Lumberjack Inputs für Linux Server sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/01-linux-input.conf
```

```
input {  
  lumberjack {  
    port => 5000  
    type => "linux"  
    ssl_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"  
    ssl_key => "/etc/pki/tls/private/logstash-forwarder.key"  
  }  
}
```

## 19.11 Logstash Windows Input Konfiguration

Zu Erstellung des Logstash GELF Inputs für Windows Server sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/02-windows-input.conf
```

```
input {  
  gelf {  
    port => 5001  
    type => "windows"  
  }  
}
```

## 19.12 Logstash Cisco Input Konfiguration

Zu Erstellung des Logstash Syslog Inputs für Cisco Netzwerkkomponenten sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/03-cisco-input.conf
```

```
input {
  syslog {
    port => 5002
    type => "cisco"
  }
}
```

## 19.13 Logstash Linux Syslog Filter Konfiguration

Zum Erstellen des Linux Syslog Filters, sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/10-linux-syslog.conf
```

```
filter {
  if [type] == "linux" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}(?:\[ %{POSINT:syslog_pid} \])?: %{GREEDYDATA:s$
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
      add_field => [ "os", "linux" ]
    }
    syslog_pri { }
    date {
      match => [ "syslog_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss"
    ]
  }
  mutate {
    replace => [ "host", "%{host}.lwb.ch" ]
  }
}
```

## 19.14 Logstash Windows Eventlog Filter Konfiguration

Zum Erstellen des Windows Eventlog Filters, sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/11-windows-eventlog.conf
```

```
filter {
  if [type] == "windows" {
    mutate {
      add_field => [ "os", "windows" ]
    }
  }
}
```

## 19.15 Logstash Cisco Syslog Filter Konfiguration

Zum Erstellen des Cisco Syslog Filters, sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/12-cisco-syslog.conf
```

```
filter {
  if [type] == "cisco" {
    grok {
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    mutate {
      add_field => [ "os", "cisco-ios" ]
    }
    dns {
      reverse => [ "host", "%{host}" ]
      action => "replace"
    }
  }
}
```

## 19.16 Logstash Graylog Output Konfiguration

Zum Erstellen des Graylog GELF Outputs, sind die nachfolgenden Anpassungen notwendig:

```
root@VMLOG1:~# nano /etc/logstash/conf.d/30-gelf-output.conf
```

```
output {
  gelf {
    host => "127.0.0.1"
    port => 12201
  }
}
```

## 19.17 Logstash Forwarder Paket erstellen

Zuerst müssen alle Abhängigkeiten zum Erstellen des Pakets installiert werden. Als erstes wird der Ruby Version Manager und die aktuelle Stable Ruby Version installiert:

```
root@VMLOG1:~# gpg --keyserver hkp://keys.gnupg.net --recv-keys
409B6B1796C275462A1703113804BB82D39DC0E3
root@VMLOG1:~# curl -sSL https://get.rvm.io | bash -s stable --ruby
```



Damit Ruby verwendet werden kann muss die SSH Session geschlossen und neu geöffnet werden.  
Anschliessend müssen weitere Abhängigkeiten installiert werden:

```
root@VMLOG1:~# apt-get install devscripts vim git
root@VMLOG1:~# apt-get build-dep golang-go
root@VMLOG1:~# gem install fpm pleaserun
```

Nun müssen die golang Quellcode- und Beschreibungsdateien heruntergeladen werden:

```
root@VMLOG1:~# mkdir go
root@VMLOG1:~# cd go
root@VMLOG1:~/go# wget
http://ftp.de.debian.org/debian/pool/main/g/golang/golang\_1.3-3.dsc
root@VMLOG1:~/go# wget
http://ftp.de.debian.org/debian/pool/main/g/golang/golang\_1.3.orig.tar.gz
root@VMLOG1:~/go# wget
http://ftp.de.debian.org/debian/pool/main/g/golang/golang\_1.3-3.debian.tar.xz
```

In einem nächsten Schritt wird der Quellcode kompiliert und in ein Debian Paket verpackt:

```
root@VMLOG1:~/go# dpkg-source -x golang_1.3-3.dsc
root@VMLOG1:~/go/golang-1.3# cd golang-1.3/
root@VMLOG1:~/go/golang-1.3# debuild -us -uc
```

Die nun erstellten Pakete müssen anschliessend installiert werden:

```
root@VMLOG1:~/go# dpkg -i golang-go_1.3-3_amd64.deb golang-src_1.3-3_amd64.deb golang-go-linux-amd64_1.3-3_amd64.deb vim-syntax-go_1.3-3_all.deb
```

Damit golang auch verwendet werden kann, müssen die benötigten Umgebungsvariablen gesetzt werden:

```
root@VMLOG1:~# mkdir -p /usr/local/go
root@VMLOG1:~# echo "export GOPATH=/usr/local/go" >>
/etc/profile.d/gopath.sh
root@VMLOG1:~# echo "export PATH=\$PATH:\$GOPATH/bin" >>
/etc/profile.d/gopath.sh
root@VMLOG1:~# source ~/.bashrc
```

Anschliessend kann das Logstash-Forwarder-Git-Repo geklont und der Quellcode kompiliert werden:

```
root@VMLOG1:~# cd /usr/src/
root@VMLOG1:/usr/src# git clone git://github.com/elasticsearch/logstash-forwarder.git
root@VMLOG1:/usr/src# cd logstash-forwarder/
root@VMLOG1:/usr/src/logstash-forwarder# go build
root@VMLOG1:/usr/src/logstash-forwarder# make deb
```



Damit das erstellte Paket auch problemlos wiedergefunden wird, wird es in den „/root/logstash-forwarder/“ Ordner kopiert, welcher zuerst erstellt werden muss:

```
root@VMLOG1:~/logstash-forwarder# mkdir /root/logstash-forwarder/  
root@VMLOG1:~/logstash-forwarder# cp logstash-forwarder_0.4.0_amd64.deb  
/root/logstash-forwarder/
```





## 19.19 Graylog Stream Konfiguration

Da nun die ersten Logs empfangen werden können, lassen sich auch die Stream Konfigurationen vornehmen. Es wurden im Graylog Webinterface unter dem Navigationspunkt Streams die nachfolgenden Streams erstellt:

### Cisco

**Description:** Logs from Cisco network devices



IO: ▶ 0 messages/second, 1 configured rule. ▲ Hide rules



os must match exactly cisco-ios  



### DFSR Error

**Description:** Logs which show a evidence of a DFSR error

IO: ▶ 0 messages/second, 3 configured rules. ▲ Hide rules

os must match exactly windows  



SourceName must match exactly DFSR  



EventType must match regular expression (ERROR|WARNING)  



### Failed SSH Logins

**Description:** Logs which show a evidence of a invalid SSH Login

IO: ▶ 2 messages/second, 3 configured rules. ▲ Hide rules

os must match exactly linux  



file must match exactly /var/log/auth.log  

message must match regular expression sshd.+Failed  

### Linux

**Description:** Logs from a Linux Server



IO: ▶ 22 messages/second, 1 configured rule. ▲ Hide rules

os must match exactly linux  

### Windows

**Description:** Logs from a Windows Server



IO: ▶ 12 messages/second, 1 configured rule. ▲ Hide rules



os must match exactly windows  

### Windows Server Crash Shutdown

**Description:** Logs which show a evidence of a Windows Server crash st

IO: ▶ 0 messages/second, 3 configured rules. ▲ Hide rules

os must match exactly windows  

EventID must match exactly 41  



Severity must match exactly CRITICAL  

Abbildung 14: Graylog Stream Konfiguration





## 19.20 Graylog Alert Konfiguration

Die Graylog Alert Konfiguration wurde gemäss dem Konzept „Graylog Alerts“ (Seite 64) umgesetzt.  
Die Konfiguration erfolgt pro Stream und ist selbsterklärend.

## 19.21 Backup

Um alle Dateien gemäss dem Backupkonzept zu sichern, wird ein Script erstellt. Das Script soll alle Daten über FTP auf ein NAS sichern. Damit dies funktioniert, werden einige Softwarepakete benötigt. Diese werden mit dem nachfolgenden Befehl installiert:

```
root@VMLOG1:~# apt-get install python-paramiko python-gobject-2 ncftp  
duplicity
```

Nun wird das Script mit dem nachfolgenden Inhalt erstellt:

```
root@VMLOG1:~# nano /bin/backup  
#!/bin/bash  
:  
/*  
 * /bin/backup is a script for managaing duplicity backups.  
 * It provivides an easy mechanism for creating, backupup, restoring,  
 * deleting and uploading encrypted backups using duplicity and ncftp  
 *  
 * Author      : Felix Imobersteg  
 * Email       : felix.imobersteg@tfbern.ch  
 * Website     : www.tfbern.ch  
 */  
,  
  
#####  
## BASE CONFIG OPTIONS                                ##  
#####  
FTP_USER=LWB\\BACKUP  
FTP_PASS=geheimesPasswort  
FTP_SERVER=nas1.lwb.ch  
  
#####  
## DUPLICITY BACKUP LOCTIONS                            ##  
## Enter locations to backup / exclude                ##  
## Multiple directories supported, space seperated    ##  
TEMP_DIR="/tmp/backup"  
BACKUP_LOCATIONS="/etc /root /home /root /bin/backup $TEMP_DIR"  
FTP_FOLDER=Backup/duplicity/vmlog1  
#####  
  
#####  
## DUPLICITY VARS                                        ##  
#####  
DUP_ARCHIVE=ftp://$FTP_USER@$FTP_SERVER/$FTP_FOLDER/  
export FTP_PASSWORD=$FTP_PASS  
#####  
  
# check ncftp, duplicity is installed
```



```
NCFTP=$(which ncftp)
DUP=$(which duplicity)
[ -z "$NCFTP" ] && { echo "ncftp doesn't appear to be installed - this is
required for script to run"; exit 1; }
[ -z "$DUP" ] && { echo "duplicity doesn't appear to be installed - this
is required for script to run"; exit 1; }

# duplicity backup
backup() {
    #Delete backups older than 180 days
    duplicity remove-older-than 180D --no-encryption --force $DUP_ARCHIVE

    #Cleanup old data
    rm -rf $TEMP_DIR
    mkdir $TEMP_DIR
    cd $TEMP_DIR

    #Get directories to backup
    INCLUDE=""
    for CDIR in $BACKUP_LOCATIONS; do
        TMP="--include ${CDIR}"
        INCLUDE=${INCLUDE}${TMP}
    done

    #Save package selections
    dpkg --get-selections > dpkg.list

    # creates full backup if older than 30 days, else does incremental
    backup
    duplicity --no-encryption --full-if-older-than 30D $INCLUDE --exclude
    '*' / $BACKUP_EXCLUDES $DUP_ARCHIVE
}

# restore duplicity backup
# file [time] destination
restore() {
    duplicity restore --no-encryption --file-to-restore $1 --time $2
    $DUP_ARCHIVE $3
}

# list files backed up
list() {
    duplicity list-current-files --no-encryption $DUP_ARCHIVE
}

# check duplicity collection-stats
status() {
    duplicity collection-status --no-encryption $DUP_ARCHIVE
}

# Main if/elif loop
if [ "$1" = "backup" ]; then
    backup
elif [ "$1" = "restore" ]; then
    restore $2 $3 $4
elif [ "$1" = "status" ]; then
    status
elif [ "$1" = "list" ]; then
    list
```



```
else
  echo "
  /bin/backup - a helper script to manage duplicity backups

  USAGE:

  /bin/backup backup                - This will backup your files and upload
them to your remote server
  /bin/backup restore [file] [time] [destination]
                                  - Restore files from your remote server
                                  - You can optionally set the time of the
file to restore
                                  - (check duplicity TIME FORMATS for
options)
  /bin/backup list                  - List files in the most recent
duplicity backup
  /bin/backup status                - Show backup status

  "
fi

## Cleanup
export FTP_USER=
export FTP_PASS=
export FTP_SERVER=
export DUP_ARCHIVE=
```

Anschliessend muss die Datei noch ausführbar gemacht werden:

```
root@VMLOG1:~# chmod 755 /bin/backup
```

Damit Script auch jede Nacht ausgeführt wird, wird ein Cronjob erstellt. Weiter wird der Output Scripts, zur Kontrolle, an [informatik@tfbern.ch](mailto:informatik@tfbern.ch) versendet:

```
root@VMLOG1:~# crontab -e

...
MAILTO=informatik@tfbern.ch
...
0 3 * * * /bin/backup backup
```

### 19.21.1 Ausführen eines manuelles Backups

Um den Backupvorgang manuell zu starten, wird der nachfolgende Befehl verwendet:

```
root@VMLOG1:~# /bin/backup backup
```



### 19.21.2 Anzeige des Backupstatus

Der aktuelle Backupstatus kann mit dem nachfolgenden Befehl angezeigt werden:

```
root@VMLOG1:~# /bin/backup status
```

### 19.21.3 Anzeige des Backupinhalts

Um alle im Backup vorhandenen Dateien anzuzeigen, wird der nachfolgende Befehl verwendet:

```
root@VMLOG1:~# /bin/backup list
```

Da der oben eingesetzte Befehl eine oft sehr lange Liste zurückliefert, ist die Benutzung von grep angebracht. Wie im nachfolgenden Beispiel für eine Suche mit dem Suchbegriff „hosts“.

```
root@VMLOG1:~# /bin/backup list | grep hosts
```

### 19.21.4 Restore einer Datei oder eines Ordners

Um eine Datei zurückzuholen, wird der nachfolgende Befehl benutzt:

```
/bin/backup restore [file] [backup-time] [destination]
```

## 19.22 Installation Postfix

Damit der Mailversand mit dem Output des Backupscripts, sowie den Graylog Benachrichtigungen auch wirklich funktioniert, muss Postfix installiert und konfiguriert werden. Dies ist mit wenigen Schritten abgeschlossen:

```
root@VMLOG1:~# sudo apt-get install postfix bsd-mailx
```

Während der Installation müssen einige Fragen beantwortet werden:

- Type of mail configuration: Satellite system
- System Mail Name: VMLOG1.lwb.ch
- SMTP relay Host: vmmail1.lwb.ch

Um ein Testmail zu versenden, kann der nachfolgende Befehl verwendet werden:

```
root@VMLOG1:~# mail -s "Testmail" informatik@tfbern.ch
```

Nach Eingabe des oben genannten Befehls kann ein Mailtext angegeben werden. Um das Mail zu versenden, muss die Tastenkombination CTRL+D gedrückt werden.



## 19.23 nginx Reverse Proxy

Die Installation ist mit dem nachfolgenden Befehl schnell erledigt:

```
root@VMLOG1:~# apt-get install nginx
```

Da für dieses Projekt nur eine sehr minimale Konfiguration benötigt wird, können zuerst einige nicht benötigte Konfigurationsdateien und Verzeichnisse gelöscht werden.

```
root@VMLOG1:~# cd /etc/nginx/  
root@VMLOG1:/etc/nginx# rm -rf sites-available/  
root@VMLOG1:/etc/nginx# rm -rf sites-enabled/  
root@VMLOG1:/etc/nginx# rm nginx.conf
```

Nun muss das „\*lwb.ch“ Wildcard Zertifikat (selbstsigniert - nur zur Verwendung für MA RI) kopiert werden. Die einfachste Möglichkeit ist es, dieses von einem anderen Server zu kopieren:

```
root@VMLOG1:/etc/nginx# mkdir ssl  
root@VMLOG1:/etc/nginx# scp -r  
root@vmweb1.lwb.ch:/etc/apache2/ssl/wildcard_lwb_ch ssl
```

In einem nächsten Schritt wird die nginx Konfiguration erstellt:

```
root@VMLOG1:/etc/nginx# nano nginx.conf  
  
user www-data;  
worker_processes 2;  
  
events {  
    worker_connections 1024;  
}  
  
http {  
  
    include mime.types;  
    default_type application/octet-stream;  
    sendfile on;  
    keepalive_timeout 65;  
  
    gzip on;  
    gzip_http_version 1.1;  
    gzip_comp_level 2;  
  
    access_log /var/log/nginx/access.log;  
    error_log /var/log/nginx/error.log;  
  
    server {  
        listen 80;  
        server_name _;  
        rewrite ^ https://$host$request_uri? permanent;  
    }  
  
    server {  
        listen 443;
```



```
ssl on;
ssl_certificate /etc/nginx/ssl/wildcard_lwb_ch/host.crt;
ssl_certificate_key
/etc/nginx/ssl/wildcard_lwb_ch/host.key;

ssl_session_timeout 10m;
ssl_prefer_server_ciphers on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers 'AES256+EECDH:AES256+EDH';
ssl_session_cache shared:SSL:10m;

location / {
    proxy_pass http://localhost:9000/;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $remote_addr;
    proxy_set_header Host $host;
}
}
```

Anschliessend muss nginx nur noch neugestartet werden.

```
root@VMLOG1:/etc/nginx# /etc/init.d/nginx restart
```

Ab diesem Zeitpunkt ist das Graylog Webinterface unter <https://log.lwb.ch> über eine verschlüsselte Verbindung verfügbar.

## 19.24 Test VM's

Zum Testen von Scripts und Konfigurationen wurden VM's verwendet. Diese wurden mit Hilfe der Software Vagrant automatisch konfiguriert. In den nachfolgenden Unterkapiteln sind die benötigten Konfigurationen ersichtlich. Informationen zur Installation und Benutzung von Vagrant sind unter <https://www.vagrantup.com/> ersichtlich.

### 19.24.1 Vagrantfile Debian Wheezy

```
#Vagrantfile Debian Wheezy
VAGRANTFILE_API_VERSION = "2"

Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|

  #Set box
  config.vm.box = "puphpet/debian75-x64"

  #Check updates
  config.vm.box_check_update = true

  #Virtual Box settings
  config.vm.provider "virtualbox" do |vb|
    # Don't boot with headless mode
  end
end
```



```
#vb.gui = true

# Set VM settings
vb.customize ["modifyvm", :id, "--memory", "512"]
vb.customize ["modifyvm", :id, "--cpus", 1]
end
end
```

### 19.24.2 Vagrantfile Windows Server 2008R2

```
#Vagrantfile Windows Server 2008R2
VAGRANTFILE_API_VERSION = "2"

Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|

  #Set box
  config.vm.box = "opentable/win-2008r2-enterprise-amd64-nocm"

  #Check updates
  config.vm.box_check_update = true

  #Windows specific settings
  config.vm.communicator = "winrm"

  #Virtual Box settings
  config.vm.provider "virtualbox" do |vb|
    #Show virtualbox gui
    vb.gui = true

    # Set VM settings
    vb.customize ["modifyvm", :id, "--memory", "2048"]
    vb.customize ["modifyvm", :id, "--cpus", 2]
    vb.customize ['modifyvm', :id, '--vram', '128']
    vb.customize ['modifyvm', :id, '--accelerate2dvideo', 'off']
    vb.customize ['modifyvm', :id, '--clipboard', 'bidirectional']
    vb.customize ["modifyvm", :id, "--draganddrop", "bidirectional"]
  end
end
```

### 19.24.3 Vagrantfile Windows Server 2012

```
#Vagrantfile Windows Server 2012
VAGRANTFILE_API_VERSION = "2"

Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|

  #Set box
  config.vm.box = "opentable/win-2012-datacenter-amd64-nocm"

  #Check updates
  config.vm.box_check_update = true

  #Windows specific settings
  config.vm.communicator = "winrm"
```



```
#Virtual Box settings
config.vm.provider "virtualbox" do |vb|
  #Show virtualbox gui
  vb.gui = true

  # Set VM settings
  vb.customize ["modifyvm", :id, "--memory", "2048"]
  vb.customize ["modifyvm", :id, "--cpus", 2]
  vb.customize ['modifyvm', :id, '--vram', '128']
  vb.customize ['modifyvm', :id, '--accelerate2dvideo', 'off']
  vb.customize ['modifyvm', :id, '--clipboard', 'bidirectional']
  vb.customize ["modifyvm", :id, "--draganddrop", "bidirectional"]
end
end
```

## 19.25 Installation sendende Windows Server

Zur Installation der sendenden Windows Server wurde der Ordner [\\vmdienst1\DCSWRepository\I\nxlog](#) erstellt, welcher alle benötigten Dateien zur Installation und Konfiguration eines sendenden Windows Servers enthält. Unter anderem wurde ein Batch mit dem Namen „install.bat“ erstellt, welche alle notwendigen Anpassungen automatisch vornimmt. Der Inhalt des Batches ist nachfolgend ersichtlich:

```
msiexec.exe /i \\vmdienst1\DCSWRepository\I\nxlog\nxlog-ce-2.8.1248.msi
/qn
net stop nxlog
copy \\vmdienst1\DCSWRepository\I\nxlog\nxlog.conf "C:\Program Files
(x86)\nxlog\conf" /Y
net start nxlog
echo "NXLog Installation abgeschlossen"
pause
```

Zur Installation eines sendenden Hosts muss lediglich die Datei „install.bat“ ausgeführt werden. Der Batch ist für Windows Server 2008R2 sowie Windows Server 2012 funktionsfähig.

## 19.26 Installation sendende Linux Server

Zur Installation der sendenden Linux Server wurde auf dem Server VMLOG1 das Verzeichnis „/root/logstash-forwarder“ angelegt. In diesem Verzeichnis befinden sich alle Dateien, welche zu Installation und Konfiguration eines sendenden Linux Server benötigt werden. Unter anderem wurde ein Bash Script mit dem Namen „install.sh“ erstellt, welches alle notwendigen Anpassungen automatisch vornimmt. Das Script ist unter Debian Wheezy funktionsfähig. Der Inhalt des Scriptes ist nachfolgend ersichtlich:

```
#!/bin/bash
cd "$(dirname "$0")"
apt-get update
dpkg -i logstash-forwarder_0.4.0_amd64.deb
cp init/logstash-forwarder /etc/init.d
cp config/logstash-forwarder /etc
mkdir -p /etc/pki/tls/certs
cp certs/logstash-forwarder.crt /etc/pki/tls/certs
update-rc.d logstash-forwarder defaults
```





```
/etc/init.d/logstash-forwarder restart
```

Um die Installation auf einem Server zu starten, kann der nachfolgende Befehl genutzt werden:

```
root@VMWEB1:~# scp -r root@vmlog1.lwb.ch:/root/logstash-forwarder /tmp &&  
sh /tmp/logstash-forwarder/install.sh && rm -rf /tmp/logstash-forwarder
```

## 19.27 Konfiguration sendende Cisco Switches

Um den Logversand auf den Cisco Switches einzuschalten, ist die nachfolgende Konfigurationsanpassung auf dem sendenden Gerät notwendig:

```
lo003-e00aa-sal#conf t  
lo003-e00aa-sal(config)#logging host 86.118.120.30 transport udp port  
5002  
lo003-e00aa-sal(config)#logging trap debugging  
lo003-e00aa-sal(config)#logging source-interface Vlan110  
lo003-e00aa-sal(config)#exit  
lo003-e00aa-sal#write
```

Damit die Anzeige des Hostnamens im Graylog Webinterface funktioniert, ist es notwendig, dass für das sendende Gerät ein funktionierender Forward und Reverse DNS Eintrag erstellt wurde.

## 19.28 Installation Logclient (VMLOG1)

Damit der Status von VMLOG1 durch die Monitoring Infrastruktur abgefragt werden kann, muss zuerst ein der Nagios NRPE Server auf dem Host VMLOG1 installiert werden. Dies geschieht mit dem nachfolgenden Befehl:

```
root@VMLOG1:~# apt-get install nagios-nrpe-server
```

Weiter werden Plugins für das Elasticsearch, Graylog und MongoDB Check inklusive den benötigten Abhängigkeiten installiert:

```
root@VMLOG1:/usr/lib/nagios/plugins# wget  
https://raw.githubusercontent.com/orthecreedence/check\_elasticsearch/master/check\_elasticsearch  
root@VMLOG1:/usr/lib/nagios/plugins# chmod 755 check_elasticsearch  
root@VMLOG1:/usr/lib/nagios/plugins# wget  
https://raw.githubusercontent.com/mzupan/nagios-plugin-mongodb/master/check\_mongodb.py  
root@VMLOG1:/usr/lib/nagios/plugins# apt-get install python-pymongo  
root@VMLOG1:/usr/lib/nagios/plugins# chmod 755 check_mongodb.py  
root@VMLOG1:~# wget https://github.com/Graylog2/check-graylog2-stream/releases/download/1.2/check-graylog2-stream.linux\_x86.tar.gz  
root@VMLOG1:~# tar -xzf check-graylog2-stream.linux_x86.tar.gz  
root@VMLOG1:~# mv check-graylog2-stream /usr/lib/nagios/plugins  
root@VMLOG1:~# rm check-graylog2-stream.linux_x86.tar.gz
```



Um Checks auf der Graylog REST Schnittstelle zu ermöglichen, wird im Graylog Webinterface unter System -> Users ein neuer Benutzer mit den nachfolgenden Angaben erstellt:

Attribut	Wert
Username	icinga
Is Admin account	Yes
Full Name	Icinga
Email Address	<a href="mailto:icinga@tfbern.ch">icinga@tfbern.ch</a>
Password	siehe Keepass

Tabelle 81: Icinga Graylog Benutzer

Anschliessend ist es notwendig einige Konfigurationsanpassungen gemäss dem TF Bern Standard vorzunehmen:

```
root@VMLOG1:~# nano /etc/nagios/nrpe.cfg

...
allowed_hosts=127.0.0.1,86.118.120.177
...
command[check_procs]=/usr/lib/nagios/plugins/check_procs -w 250 -c 400
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w '20%' -c
'10%' -e
command[check_elasticsearch]=/usr/lib/nagios/plugins/check_elasticsearch
command[check_mongodb]=/usr/lib/nagios/plugins/check_mongodb.py
command[check_graylog-web]=/usr/lib/nagios/plugins/check_http -H
127.0.0.1 -p 9000
command[check_graylog-stream-crash-
shutdown]=/usr/lib/nagios/plugins/check-graylog2-stream -user=icinga -
password=geheimesPasswort -stream=54e4a8dbe4b0b1310bb74e1c
command[check_graylog-stream-failed-ssh]=/usr/lib/nagios/plugins/check-
graylog2-stream -user=icinga -password= geheimesPasswort -
stream=54e4a64ce4b0b1310bb74b53
command[check_graylog-stream-dfsr-error]=/usr/lib/nagios/plugins/check-
graylog2-stream -user=icinga -password= geheimesPasswort -
stream=54e4a4fce4b0b1310bb749e4
...
```

Damit alle eben erfolgten Änderungen übernommen werden, muss der Nagios NRPE Server Dienst neu gestartet werden:

```
root@VMLOG1:~# /etc/init.d/nagios-nrpe-server restart
```

## 19.29 Konfiguration Icinga

Um das Monitoring zu aktivieren, müssen einige Änderungen an der bestehenden Icinga Konfiguration vorgenommen werden. **Achtung:** Alle Änderungen in diesem Kapitel werden auf dem Server VMON1 durchgeführt.

### 19.29.1 Hostgruppe Logserver

Zuerst muss die Hostgruppe für Logserver erstellt werden, damit später die auszuführenden Servicechecks zugewiesen werden können. Die Gruppe wird mit den nachfolgenden Schritten erstellt:

```
root@VMMON1:/etc/icinga/objects# nano g_log-servers_icinga.cfg
```

```
define hostgroup {  
    hostgroup_name g_log-servers  
    alias Log-Servers  
}
```

### 19.29.2 Host VMLOG1

In einem nächsten Schritt muss ein Hostobjekt für den Server VMLOG1 erstellt werden.

```
root@VMMON1:/etc/icinga/objects# nano h_vmlog1_icinga.cfg
```

```
define host{  
    use t_debian-server  
    host_name vmlog1  
    alias vmlog1  
    address 86.118.120.30  
    hostgroups g_debian-servers,g_http-servers,g_https-  
servers,g_log-servers  
}
```

### 19.29.3 Serviceobjekte VMLOG1

In einem nächsten Schritt müssen die benötigten Serviceobjekte erstellt werden, welche auf für den Server VMLOG1 verwendet werden:

```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-mongodb_icinga.cfg
```

```
define service{  
    use t_default-service  
    hostgroup_name g_log-servers  
    service_description MongoDB  
    check_command check_nrpe_larg!check_mongodb  
}
```

```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-elasticsearch_icinga.cfg
```

```
define service{  
    use t_default-service  
    hostgroup_name g_log-servers  
    service_description Elasticsearch  
    check_command check_nrpe_larg!check_elasticsearch  
}
```



```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-graylog-web_icinga.cfg
```

```
define service{
    use                t_default-service
    hostgroup_name      g_log-servers
    service_description Graylog Web
    check_command        check_nrpe_larg!check_graylog-web
}
```

```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-graylog-stream-crash-
shutdown_icinga.cfg
```

```
define service{
    use                t_default-service
    hostgroup_name      g_log-servers
    service_description Graylog Stream Windows Server
    Crash Shutdown Alert
    check_command        check_nrpe_larg!check_graylog-
stream-crash-shutdown
}
```

```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-graylog-stream-failed-
ssh_icinga.cfg
```

```
define service{
    use                t_default-service
    hostgroup_name      g_log-servers
    service_description Graylog Stream Failed SSH Logins
    Alert
    check_command        check_nrpe_larg!check_graylog-
stream-failed-ssh
}
```

```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-graylog-stream-dfsr-
error_icinga.cfg
```

```
define service{
    use                t_default-service
    hostgroup_name      g_log-servers
    service_description Graylog Stream DFSR Error Alert
    check_command        check_nrpe_larg!check_graylog-
stream-dfsr-error
}
```

#### 19.29.4 Checks sendende Windows Server

In einem nächsten Schritt wird ein neues Kommando erstellt, bei welchem überprüft wird, ob der Prozess nxlog.exe auf allen Windows Server läuft:

```
root@VMMON1:/etc/icinga/objects# nano c_commands_icinga.cfg
```

```
define command {
    command_name      check_nxlog
    command_line       /usr/lib/nagios/plugins/check_nt -H $HOSTADDRESS$
-s geheimesPasswort -p 12489 -v PROCSTATE -d SHOWALL -l nxlog.exe
}
```

Anschliessend muss noch das zugehörige Service Objekt erstellt werden:

```
root@VMMON1:/etc/icinga/objects# nano s_nsclient-nxlog_icinga.cfg
```

```
define service{
    use                t_default-service
    hostgroup_name      g_windows-servers
    service_description NXLog Process
    check_command        check_nxlog
}
```

### 19.29.5 Checks sendende Linux Server

Unter Linux Servern wird überprüft, ob ein Prozess mit dem Name „logstash-forwarder“ läuft. Leider wurde hierfür kein passendes Plugin gefunden, welcher diesen Check ermöglicht. Aus diesem Grund wurde ein eigenes Plugin erstellt:

```
root@VMMON1:~# nano /usr/lib/nagios/plugins/check_logstash-forwarder
```

```
#!/bin/bash
ps=`ps aux`
process_count=`echo $ps | grep -c "/opt/logstash-forwarder/bin/logstash-
forwarder -config /etc/logstash-forwarder"`
if [ $process_count -gt 0 ]
then
    echo "OK - Logstash Forwarder is running"
    exit 0
fi

echo "CRITICAL - Logstash Forwarder is not running"
exit 2
```

Das obenstehende Script muss auf alle zu überprüfenden Server kopiert werden. Weiter muss die Nagios NRPE Konfiguration auf den zu überprüfenden Server angepasst werden:

```
root@VMMON1:~# nano /etc/nagios/nrpe.cfg
```

```
...
command[check_logstash-forwarder]=/usr/lib/nagios/plugins/check_logstash-
forwarder
...
```

Nun muss lediglich noch ein Service Objekt erstellt werden:

```
root@VMMON1:/etc/icinga/objects# nano s_nrpe-logstash-
forwarder_icinga.cfg
```

```
define service{
    use                t_default-service
    hostgroup_name      g_debian-servers
    service_description Logstash-Forwarder
    check_command        check_nrpe_larg!check_logstash-
forwarder
}
```



## 19.29.6 Abschluss der Konfiguration

Damit die Konfigurationsänderungen übernommen werden, muss der Icinga Service neu gestartet werden:

```
root@VMMON1:~# /etc/init.d/icinga restart
```

## 19.30 Aufgetretene Probleme

Die nachfolgenden Unterkapitel zeigen Probleme, die Ursachen und deren Lösung, welche während der Realisation aufgetreten sind.

### 19.30.1 MongoDB: Connection Refused

#### 19.30.1.1 Beschreibung

Nach der Installation von MongoDB ereignet sich folgender Fehler:

```
root@VMLOG1:~# mongo
MongoDB shell version: 2.6.7
connecting to: test
2015-02-17T10:17:44.933+0100 warning: Failed to connect to
127.0.0.1:27017, reason: errno:111 Connection refused
2015-02-17T10:17:44.934+0100 Error: couldn't connect to server
127.0.0.1:27017 (127.0.0.1), connection attempt failed at
src/mongo/shell/mongo.js:146
exception: connect failed
```

Gleichzeitig liefert MongoDB das Init Script den folgenden Status zurück:

```
root@VMLOG1:~# /etc/init.d/mongod status
[ ok ] Checking status of database: mongod running.
```

#### 19.30.1.2 Ursache

MongoDB ist nicht sauber gestartet.

#### 19.30.1.3 Lösung

Neustart von MongoDB mit:

```
root@VMLOG1:~# /etc/init.d/mongod restart
```

## 19.30.2 Graylog-Server: Startet nicht

### 19.30.2.1 Beschreibung

Der Graylog Server Dienst wird nicht gestartet, obwohl beim Ausführen des Init-Scripts kein Fehler erscheint. Im Log ist der folgende Fehler zu finden:

```
root@VMLOG1:~# tail -100 /var/log/graylog2-server/console.log
Exception in thread "main" java.io.IOException: java.io.IOException: Parent
folder is not writable: /var/lib/graylog2-server/message-cache-
spool/input-cache
    at org.mapdb.Volume$MappedFileVol.<init>(Volume.java:439)
    at org.mapdb.Volume.volumeForFile(Volume.java:176)
    at org.mapdb.Volume$1.createIndexVolume(Volume.java:203)
    at org.mapdb.StoreDirect.<init>(StoreDirect.java:202)
    at org.mapdb.StoreWAL.<init>(StoreWAL.java:74)
    at org.mapdb.DBMaker.extendStoreWAL(DBMaker.java:928)
    at org.mapdb.DBMaker.makeEngine(DBMaker.java:722)
    at org.mapdb.DBMaker.make(DBMaker.java:665)
    ...
```

### 19.30.2.2 Ursache

Fehlende Schreibberechtigung im Verzeichnis „/var/lib/graylog2-server/“ für Everyone.

### 19.30.2.3 Lösung

Manuelles Setzen der Berechtigung und Neustart des Graylog Server Dienstes

```
root@VMLOG1:~# chmod -R 777 /var/lib/graylog2-server
root@VMLOG1:~# /etc/init.d/graylog2-server restart
```

## 19.30.3 Kein funktionierendes Debian-Paket für Logstash Forwarder vorhanden

### 19.30.3.1 Beschreibung

Im Logstash bzw. Elasticsearch Repository ist die paketierte Logstash-Forwarder Version für Debian nicht mehr verfügbar.

### 19.30.3.2 Ursache

Aufgrund eines grösseren Bugs des Pakets von Logstash-Forwarder wurde die paketierte Version durch das Entwicklerteam gelöscht,

### 19.30.3.3 Lösung

Erstellen eines eigenen Paketes. Siehe Kapitel „Logstash Forwarder Paket erstellen“ (Seite 101)

## 19.30.4 Kein Logempfang von Cisco Routern

### 19.30.4.1 Beschreibung

Es werden keine Logs von Cisco Routern empfangen.

### 19.30.4.2 Ursache

Auf den Routern ist das Logging Interface nicht auf „Vlan190“ gesetzt. Leider lässt sich das Logging Interface auf den Routern nicht auf „Vlan190“ schalten. Es lässt sich nur das verwendete VRF oder ein globales Interface wählen. Allerdings werden auch auf diese Weise die Logs nicht empfangen.

### 19.30.4.3 Lösung

Es wurde keine funktionierende Lösung gefunden. Da die Durchführung der benötigten Arbeiten am Backbone des produktiven Systems zu gefährlich wären, lässt sich dieses Problem nicht während der IPA beheben. Gemeinsam mit dem Fachvorgesetzten wurde die Entscheidung getroffen, dieses Problem nicht weiter zu verfolgen, da der Nutzen in keinem Verhältnis zum Risiko eines Ausfalls und dem Aufwand steht.

## 19.31 Testprotokoll

In diesem Kapitel sind die Ergebnisse der durchgeführten Tests zu finden. Sämtliche Tests stützen sich auf das erarbeitete Testkonzept (Seite 75).

### 19.31.1 Funktionelle Anwendertests

#### 19.31.1.1 Testfall TF1 (Zugriff Graylog Web funktioniert)

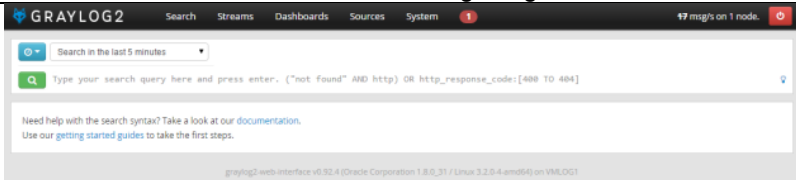
Testfall TF1	
<b>Testobjekte</b>	TO2, TO3, TO4, TO9, TO10, F2
<b>Systemziele / Anforderungen</b>	S1, S2
<b>Testbeschreibung</b>	Graylog Webinterface kann angezeigt werden
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Öffnen eines Browsers</li> <li>2. Öffnen der URL <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>3. Login mit SHH Domänenaccount</li> </ol>
<b>Erwartet (Soll)</b>	Webinterface wird ohne Fehler angezeigt
<b>Erwartet (Ist)</b>	Das Webinterface wird ohne Fehler angezeigt.
<b>Kommentar / Screenshot</b>	 <p>Abbildung 15: TF1 Screenshot</p>

Tabelle 82: Testfall TF1 (Zugriff Graylog Web funktioniert)



### 19.31.1.2 Testfall TF2 (Installationsscript Windows Server 2008R2 funktioniert)

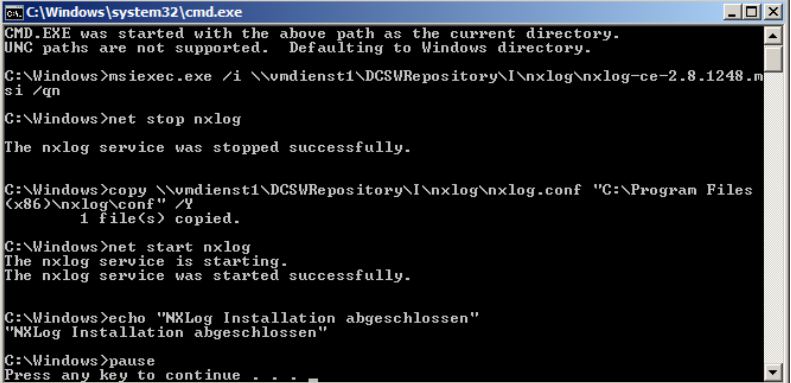
Testfall TF2	
Testobjekte	TO7
Systemziele / Anforderungen	S10, F7
Testbeschreibung	Das Script zur automatischen Konfiguration eines sendenden Windows Servers 2008R2 funktioniert.
Testvorgehen	<ol style="list-style-type: none"> <li>1. Starten einer VM mit der Grundinstallation von Windows Server 2008R2</li> <li>2. Ausführen des Installationsscript</li> <li>3. 3min warten</li> </ol>
Erwartet (Soll)	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
Erwartet (Ist)	Das Script wird ohne Fehler ausgeführt. Nach 3min Wartezeit sind die Logs unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
Kommentar / Screenshot	 <p>Abbildung 16: TF2 Screenshot</p>

Tabelle 83: Testfall TF2 (Installationsscript Windows Server 2008R2 funktioniert)

### 19.31.1.3 Testfall TF3 (Installationsscript Windows Server 2012 funktioniert)

Testfall TF3	
Testobjekte	TO7
Systemziele / Anforderungen	S10, F7
Testbeschreibung	Das Script zur automatischen Konfiguration eines sendenden Windows Servers 2012 funktioniert.
Testvorgehen	<ol style="list-style-type: none"> <li>1. Starten einer VM mit der Grundinstallation von Windows Server 2012</li> <li>2. Ausführen des Installationsscript</li> <li>3. 3min warten</li> </ol>
Erwartet (Soll)	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
Erwartet (Ist)	Das Script wird ohne Fehler ausgeführt. Nach 3min Wartezeit sind die Logs unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.

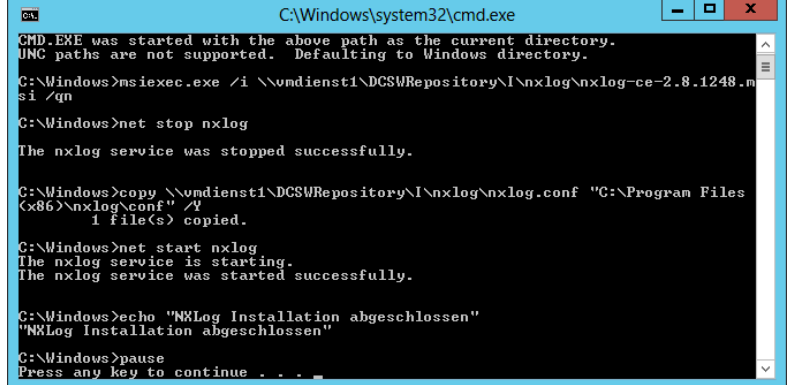
<b>Kommentar / Screenshot</b>	
-------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Abbildung 17: TF3 Screenshot

Tabelle 84: Testfall TF3 (Installationsscript Windows Server 2012 funktioniert)

#### 19.31.1.4 Testfall TF4 (Installationsscript Linux Server funktioniert)

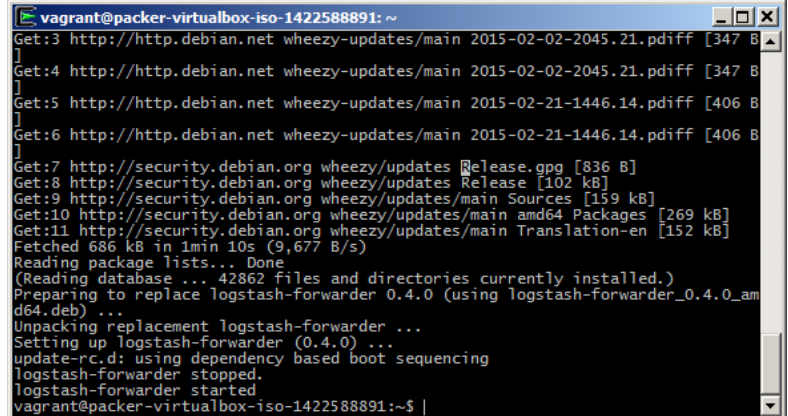
Testfall TF4	
<b>Testobjekte</b>	TO8
<b>Systemziele / Anforderungen</b>	S10, F7
<b>Testbeschreibung</b>	Das Script zur automatischen Konfiguration eines sendenden Linux Servers funktioniert.
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Starten einer VM mit der Grundinstallation von Debian Wheezy</li> <li>2. Ausführen des Installationsscript</li> <li>3. 3min warten</li> </ol>
<b>Erwartet (Soll)</b>	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
<b>Erwartet (Ist)</b>	Das Installationsscript läuft ohne Fehler durch und nach einer Wartezeit von 3min sind die ersten Logs des neu installierten Hosts unter <a href="https://log.lwb.ch">https://log.lwb.ch</a> ersichtlich.
<b>Kommentar / Screenshot</b>	

Abbildung 18: TF4 Screenshot

Tabelle 85: Testfall TF4 (Installationsscript Linux Server funktioniert)



#### 19.31.1.5 Testfall TF5 (Backup funktioniert)

Testfall TF5	
Testobjekte	TO6
Systemziele / Anforderungen	S6
Testbeschreibung	Das Backup der wichtigsten Konfigurationsdateien von VMLOG1 funktioniert.
Testvorgehen	<ol style="list-style-type: none"><li>1. SSH Login auf VMLOG1</li><li>2. Restore vom gestrigen Tag vom File /etc/hosts mit dem Script in /bin/backup</li></ol>
Erwartet (Soll)	Datei wurde zurückgeholt
Erwartet (Ist)	Datei wurde erfolgreich zurückgeholt.
Kommentar / Screenshot	<pre>root@VMLOG1:~# /bin/backup restore etc/hosts 2015-02-22 hosts NcFTP version is 3.2.5 Local and Remote metadata are synchronized, no sync needed. Last full backup date: Wed Feb 18 13:52:59 2015 root@VMLOG1:~# ls hosts  logstash-forwarder  mail</pre>

Tabelle 86: Testfall TF5 (Backup funktioniert)

#### 19.31.1.6 Testfall TF6 (Sendende Linux Server hinzugefügt)























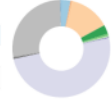












































Testfall TF6																																																																												
Testobjekte	TO11																																																																											
Systemziele / Anforderungen	S8, F15																																																																											
Testbeschreibung	Alle sendenden Linuxserver wurden konfiguriert und deren Lognachrichten sind in Graylog ersichtlich.																																																																											
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Klick auf Sources in der Navigation</li><li>3. Setzen des Zeitlimit auf die letzten 30 Tage</li></ol>																																																																											
Erwartet (Soll)	Alle Linux Server aus der Anforderung F15 sind hinzugefügt und in der Sources-Übersicht ersichtlich.																																																																											
Erwartet (Ist)	Alle Linux Server wurden hinzugefügt.																																																																											
Kommentar / Screenshot	<div><table><tr><th>Source name</th><th>Percentage</th><th>Message count</th></tr><tr><td colspan="3">Top Sources</td></tr><tr><td> <a href="#">vmmail1.lwb.ch</a></td><td>50.02%</td><td>54891</td></tr><tr><td> <a href="#">vmprint1.lwb.ch</a></td><td>27.39%</td><td>30058</td></tr><tr><td> <a href="#">vmdc1.lwb.ch</a></td><td>13.56%</td><td>14880</td></tr><tr><td colspan="3">Others</td></tr><tr><td> <a href="#">vmdc2.lwb.ch</a></td><td>2.94%</td><td>3229</td></tr><tr><td> <a href="#">ghdr1.lwb.ch</a></td><td>2.90%</td><td>3183</td></tr><tr><td> <a href="#">vmdienst1.lwb.ch</a></td><td>0.65%</td><td>710</td></tr><tr><td> <a href="#">vmorga1.lwb.ch</a></td><td>0.41%</td><td>445</td></tr><tr><td> <a href="#">vmdb1.lwb.ch</a></td><td>0.37%</td><td>401</td></tr><tr><td> <a href="#">vmmon1.lwb.ch</a></td><td>0.35%</td><td>379</td></tr><tr><td> <a href="#">vmfile1.lwb.ch</a></td><td>0.30%</td><td>327</td></tr><tr><td> <a href="#">vmfai1.lwb.ch</a></td><td>0.26%</td><td>285</td></tr><tr><td> <a href="#">vmfyt1.lwb.ch</a></td><td>0.25%</td><td>271</td></tr><tr><td> <a href="#">vmweb1.lwb.ch</a></td><td>0.15%</td><td>163</td></tr><tr><td> <a href="#">vmveeam1.lwb.ch</a></td><td>0.11%</td><td>118</td></tr><tr><td> <a href="#">ghbackup1.lwb.ch</a></td><td>0.09%</td><td>100</td></tr><tr><td> <a href="#">vagrant-2008r23.lwb.ch</a></td><td>0.07%</td><td>80</td></tr><tr><td> <a href="#">ghic1.lwb.ch</a></td><td>0.06%</td><td>71</td></tr><tr><td> <a href="#">vmem1.lwb.ch</a></td><td>0.04%</td><td>43</td></tr><tr><td> <a href="#">vmlog1.lwb.ch</a></td><td>0.03%</td><td>35</td></tr><tr><td> <a href="#">vagrant-20123.lwb.ch</a></td><td>0.02%</td><td>24</td></tr><tr><td> <a href="#">vmis1.lwb.ch</a></td><td>0.02%</td><td>21</td></tr><tr><td> <a href="#">packer-virtualbox-iso-142588891.lwb.ch</a></td><td>0.01%</td><td>16</td></tr></table></div>	Source name	Percentage	Message count	Top Sources			 <a href="#">vmmail1.lwb.ch</a>	50.02%	54891	 <a href="#">vmprint1.lwb.ch</a>	27.39%	30058	 <a href="#">vmdc1.lwb.ch</a>	13.56%	14880	Others			 <a href="#">vmdc2.lwb.ch</a>	2.94%	3229	 <a href="#">ghdr1.lwb.ch</a>	2.90%	3183	 <a href="#">vmdienst1.lwb.ch</a>	0.65%	710	 <a href="#">vmorga1.lwb.ch</a>	0.41%	445	 <a href="#">vmdb1.lwb.ch</a>	0.37%	401	 <a href="#">vmmon1.lwb.ch</a>	0.35%	379	 <a href="#">vmfile1.lwb.ch</a>	0.30%	327	 <a href="#">vmfai1.lwb.ch</a>	0.26%	285	 <a href="#">vmfyt1.lwb.ch</a>	0.25%	271	 <a href="#">vmweb1.lwb.ch</a>	0.15%	163	 <a href="#">vmveeam1.lwb.ch</a>	0.11%	118	 <a href="#">ghbackup1.lwb.ch</a>	0.09%	100	 <a href="#">vagrant-2008r23.lwb.ch</a>	0.07%	80	 <a href="#">ghic1.lwb.ch</a>	0.06%	71	 <a href="#">vmem1.lwb.ch</a>	0.04%	43	 <a href="#">vmlog1.lwb.ch</a>	0.03%	35	 <a href="#">vagrant-20123.lwb.ch</a>	0.02%	24	 <a href="#">vmis1.lwb.ch</a>	0.02%	21	 <a href="#">packer-virtualbox-iso-142588891.lwb.ch</a>	0.01%	16
Source name	Percentage	Message count																																																																										
Top Sources																																																																												
 <a href="#">vmmail1.lwb.ch</a>	50.02%	54891																																																																										
 <a href="#">vmprint1.lwb.ch</a>	27.39%	30058																																																																										
 <a href="#">vmdc1.lwb.ch</a>	13.56%	14880																																																																										
Others																																																																												
 <a href="#">vmdc2.lwb.ch</a>	2.94%	3229																																																																										
 <a href="#">ghdr1.lwb.ch</a>	2.90%	3183																																																																										
 <a href="#">vmdienst1.lwb.ch</a>	0.65%	710																																																																										
 <a href="#">vmorga1.lwb.ch</a>	0.41%	445																																																																										
 <a href="#">vmdb1.lwb.ch</a>	0.37%	401																																																																										
 <a href="#">vmmon1.lwb.ch</a>	0.35%	379																																																																										
 <a href="#">vmfile1.lwb.ch</a>	0.30%	327																																																																										
 <a href="#">vmfai1.lwb.ch</a>	0.26%	285																																																																										
 <a href="#">vmfyt1.lwb.ch</a>	0.25%	271																																																																										
 <a href="#">vmweb1.lwb.ch</a>	0.15%	163																																																																										
 <a href="#">vmveeam1.lwb.ch</a>	0.11%	118																																																																										
 <a href="#">ghbackup1.lwb.ch</a>	0.09%	100																																																																										
 <a href="#">vagrant-2008r23.lwb.ch</a>	0.07%	80																																																																										
 <a href="#">ghic1.lwb.ch</a>	0.06%	71																																																																										
 <a href="#">vmem1.lwb.ch</a>	0.04%	43																																																																										
 <a href="#">vmlog1.lwb.ch</a>	0.03%	35																																																																										
 <a href="#">vagrant-20123.lwb.ch</a>	0.02%	24																																																																										
 <a href="#">vmis1.lwb.ch</a>	0.02%	21																																																																										
 <a href="#">packer-virtualbox-iso-142588891.lwb.ch</a>	0.01%	16																																																																										

Abbildung 19: TF6 Screenshot

Tabelle 87: Testfall TF6 (Sendende Linux Server hinzugefügt)



#### 19.31.1.7 Testfall TF7 (Sendende Windows Server hinzugefügt)

Testfall TF7	
Testobjekte	TO12
Systemziele / Anforderungen	S8, F14
Testbeschreibung	Alle sendenden Windowsserver wurden konfiguriert und deren Lognachrichten sind in Graylog ersichtlich.
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Klick auf Sources in der Navigation</li><li>3. Setzen des Zeitlimit auf die letzten 30 Tage</li></ol>
Erwartet (Soll)	Alle Windows Server aus der Anforderung F14 sind hinzugefügt und in der Sources-Übersicht ersichtlich.
Erwartet (Ist)	Alle Linux Windows wurden hinzugefügt.
Kommentar / Screenshot	Siehe TF 6.

Tabelle 88: Testfall TF7 (Sendende Windows Server hinzugefügt)

#### 19.31.1.8 Testfall TF8 (Sendende Netzwerkkomponenten hinzugefügt)

Testfall TF8	
Testobjekte	TO13
Systemziele / Anforderungen	S8, F16
Testbeschreibung	Alle sendenden Netzwerkkomponenten wurden konfiguriert und deren Lognachrichten sind in Graylog ersichtlich.
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li><li>2. Klick auf Sources in der Navigation</li><li>3. Setzen des Zeitlimit auf die letzten 30 Tage</li></ol>
Erwartet (Soll)	Alle Netzwerkkomponenten aus der Anforderung F16 sind hinzugefügt und in der Sources-Übersicht ersichtlich.
Erwartet (Ist)	Alle Switches wurden hinzugefügt. Die Router konnten aufgrund von Problemen bei der Konfiguration nicht hinzugefügt werden. Siehe Kapitel „Kein Logempfang von Cisco Routern“ (Seite 120)
Kommentar / Screenshot	Siehe TF 6.

Tabelle 89: Testfall TF8 (Sendende Netzwerkkomponenten hinzugefügt)

#### 19.31.1.9 Testfall TF9 (Monitoring VMLOG1 ersichtlich)

Testfall TF9	
Testobjekte	TO5
Systemziele / Anforderungen	S7, F6
Testbeschreibung	Das Monitoring ist eingerichtet und im Icinga ersichtlich
Testvorgehen	<ol style="list-style-type: none"><li>1. Öffnen von <a href="https://vmmon1.lwb.ch/icinga-web/">https://vmmon1.lwb.ch/icinga-web/</a></li><li>2. Suchen nach VMLOG1</li></ol>
Erwartet (Soll)	Der Server VMLOG1 wird gemäss Monitoring-Konzept (Seite 70) überwacht.
Erwartet (Ist)	Sämtliche Checks werden gemäss dem Monitoring-Konzept durchgeführt und sind im Icinga Webinterface ersichtlich.

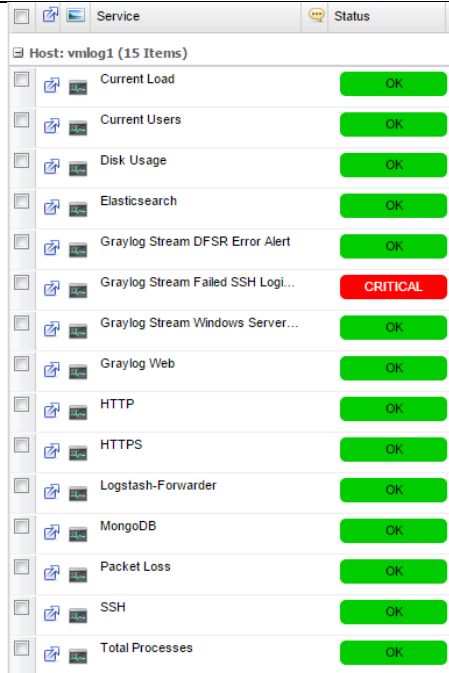
Kommentar / Screenshot	 <p>Abbildung 20: TF9 Screenshot</p>
------------------------	------------------------------------------------------------------------------------------------------------------------

Tabelle 90: Testfall TF9 (Monitoring VMLOG1 ersichtlich)

#### 19.31.1.10 Testfall TF10 (Graylog Streams eingerichtet)

Testfall TF10	
Testobjekte	TO2, TO3, TO4, TO9, TO10
Systemziele / Anforderungen	S1, S2, S9, F2, F3, F10, F11, F12
Testbeschreibung	Die Graylog Streams wurden inklusive der Alarmierung eingerichtet.
Testvorgehen	<ol style="list-style-type: none"> <li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>2. Klick auf Streams in der Navigation</li> </ol>
Erwartet (Soll)	<p>Die nachfolgenden Streams sind in der Übersicht vorhanden:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> <li>• Cisco</li> <li>• Ungültige SSH Logins</li> <li>• Windows Server Crash Shutdown</li> </ul> <p>Weiter sind die nachfolgenden Alarme ersichtlich.</p> <ul style="list-style-type: none"> <li>• DFSR Fehler</li> <li>• Ungültige SSH Logins</li> <li>• Windows Server Crash Shutdown</li> </ul>
Erwartet (Ist)	Die geforderten Streams und Alarme sind ersichtlich.

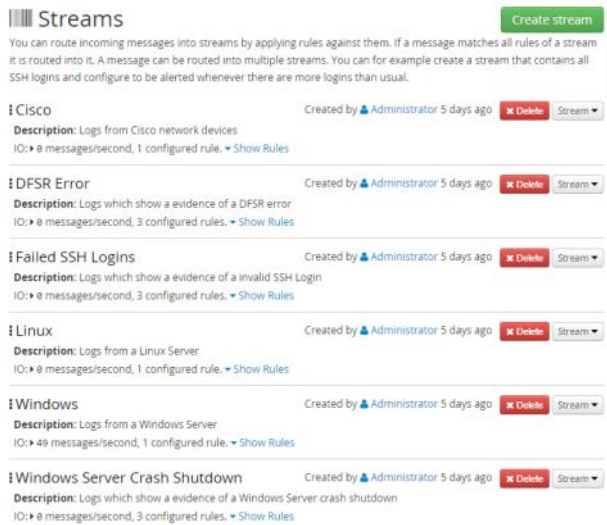
<b>Kommentar / Screenshot</b>	 <p><b>Streams</b></p> <p>You can route incoming messages into streams by applying rules against them. If a message matches all rules of a stream it is routed into it. A message can be routed into multiple streams. You can for example create a stream that contains all SSH logins and configure to be alerted whenever there are more logins than usual.</p> <p><b>Cisco</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Stream</a></p> <p><b>Description:</b> Logs from Cisco network devices IO: 0 messages/second, 1 configured rule. <a href="#">Show Rules</a></p> <p><b>DFSR Error</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Stream</a></p> <p><b>Description:</b> Logs which show a evidence of a DFSR error IO: 0 messages/second, 3 configured rules. <a href="#">Show Rules</a></p> <p><b>Failed SSH Logins</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Stream</a></p> <p><b>Description:</b> Logs which show a evidence of a invalid SSH Login IO: 0 messages/second, 3 configured rules. <a href="#">Show Rules</a></p> <p><b>Linux</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Stream</a></p> <p><b>Description:</b> Logs from a Linux Server IO: 0 messages/second, 1 configured rule. <a href="#">Show Rules</a></p> <p><b>Windows</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Stream</a></p> <p><b>Description:</b> Logs from a Windows Server IO: 49 messages/second, 1 configured rule. <a href="#">Show Rules</a></p> <p><b>Windows Server Crash Shutdown</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Stream</a></p> <p><b>Description:</b> Logs which show a evidence of a Windows Server crash shutdown IO: 0 messages/second, 3 configured rules. <a href="#">Show Rules</a></p> <p><b>Abbildung 21: TF10 Screenshot</b></p>
-------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabelle 91: Testfall TF10 (Graylog Streams eingerichtet)

#### 19.31.1.11 Testfall TF11 (Graylog Übersichtsdashboard eingerichtet)

Testfall TF 11	
<b>Testobjekte</b>	TO2, TO3, TO4, TO9, TO10
<b>Systemziele / Anforderungen</b>	S1, S2, F2, F13
<b>Testbeschreibung</b>	Das Graylog Übersichtsdashboard ist eingerichtet
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>Klick auf „Dashboards“ in der Navigation</li> </ol>
<b>Erwartet (Soll)</b>	Es ist ein Dashboard mit den wichtigsten Kennzahlen verfügbar.
<b>Erwartet (Ist)</b>	Das Übersichtsdashboard ist vorhanden.
<b>Kommentar / Screenshot</b>	 <p><b>Dashboards</b></p> <p>Use dashboards to create specific views on your messages. Create a new dashboard here and add any graph or chart you create in other parts of Graylog2 with one click.</p> <p><b>Main</b> Created by Administrator 5 days ago <a href="#">Delete</a> <a href="#">Set as start page</a></p> <p>6 widgets. Main Dashboard</p> <p><b>Abbildung 22: TF11 Screenshot</b></p>

Tabelle 92: Testfall TF11 (Graylog Übersichtsdashboard eingerichtet)

### 19.31.2 Nicht funktionale Anwendertests

#### 19.31.2.1 Testfall TF12 (Schneller Zugriff auf Webinterface)

Testfall TF 12	
<b>Testobjekte</b>	TO2, TO3, TO4, TO9, TO10
<b>Systemziele / Anforderungen</b>	NF2
<b>Testbeschreibung</b>	Dieser Test stellt sicher, dass der Zugriff auf das Graylog Webinterface schnell möglich ist
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a> im Google Chrome</li> <li>Öffnen der Developer Tools (F12)</li> <li>Klick auf Network in den Developer Tools</li> <li>Suche nach allen Logs in den letzten 5min</li> </ol>

<b>Erwartet (Soll)</b>	Die Ladezeit beträgt weniger als 5s
<b>Erwartet (Ist)</b>	Die Ladezeit beträgt 1.81s.
<b>Kommentar / Screenshot</b>	<p><b>Abbildung 23: TF12 Screenshot</b></p>

Tabelle 93: Testfall TF12 (Schneller Zugriff auf Webinterface)

### 19.31.3 Sicherheitstest

#### 19.31.3.1 Testfall TF13 (Anmeldung für Mitglieder G\_MA-INF)

<b>Testfall TF 13</b>	
<b>Testobjekte</b>	TO2, TO3, TO4, TO9, TO10
<b>Systemziele / Anforderungen</b>	F8, F9
<b>Testbeschreibung</b>	Dieser Test stellt sicher, dass sich ein Benutzer, mit Mitgliedschaft in der Gruppe G_MA-INF, am Graylog Webinterface anmelden kann.
<b>Testvorgehen</b>	<ol style="list-style-type: none"> <li>1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a></li> <li>2. Login mit dem Benutzer SHH</li> </ol>
<b>Erwartet (Soll)</b>	Login erfolgreich
<b>Erwartet (Ist)</b>	Das Login funktioniert wie gewünscht.
<b>Kommentar / Screenshot</b>	Kein

Tabelle 94: Testfall TF13 (Anmeldung für Mitglieder G\_MA-INF)

#### 19.31.3.2 Testfall TF14 (Anmeldung für Nicht-Mitglieder G\_MA-INF)

<b>Testfall TF 14</b>	
<b>Testobjekte</b>	TO2, TO3, TO4, TO9, TO10
<b>Systemziele / Anforderungen</b>	F8, F9
<b>Testbeschreibung</b>	Dieser Test stellt sicher, dass sich ein Benutzer, welcher nicht Mitglied der Gruppe G_MA-INF ist, sich nicht am Graylog Webinterface anmelden kann.

<b>Testvorgehen</b>	1. Öffnen von <a href="https://log.lwb.ch">https://log.lwb.ch</a> 2. Login mit dem Benutzer TEST-V
<b>Erwartet (Soll)</b>	Login schlägt mit Fehlermeldung fehl.
<b>Erwartet (Ist)</b>	Das Login schlägt wie gewünscht fehl.
<b>Kommentar / Screenshot</b>	 <p>Abbildung 24: TF14 Screenshot</p>

Tabelle 95: Testfall TF14 (Anmeldung für Nicht-Mitglieder G\_MA-INF)

#### 19.31.3.3 Testfall TF15 (Webinterface ist verschlüsselt)

<b>Testfall TF15</b>	
<b>Testobjekte</b>	TO3, TO4
<b>Systemziele / Anforderungen</b>	S2, F4
<b>Testbeschreibung</b>	Dieser Test stellt sicher, dass der Zugriff auf das Webinterface verschlüsselt erfolgt.
<b>Testvorgehen</b>	1. Öffnen von <a href="http://log.lwb.ch">http://log.lwb.ch</a>
<b>Erwartet (Soll)</b>	Der Benutzer wird automatisch von <a href="http://log.lwb.ch">http://log.lwb.ch</a> nach <a href="https://log.lwb.ch">https://log.lwb.ch</a> weitergeleitet. Es erscheint keinerlei Fehler, welcher die Verschlüsselung betrifft.
<b>Erwartet (Ist)</b>	Beim Aufruf der Seite <a href="http://log.lwb.ch">http://log.lwb.ch</a> wird man automatisch nach <a href="https://log.lwb.ch">https://log.lwb.ch</a> weitergeleitet.
<b>Kommentar / Screenshot</b>	Kein

Tabelle 96: Testfall TF15 (Anmeldung für Nicht-Mitglieder G\_MA-INF)

### 19.31.4 Fehlerprotokolle

#### 19.31.4.1 Fehlerprotokoll 1

<b>Fehlerprotokoll</b>	
<b>Testfall ID</b>	TF8
<b>Fehlerbeschreibung</b>	Die Cisco Router wurden nicht hinzugefügt. Siehe Kapitel „Kein Logempfang von Cisco Routern“ (Seite 120)
<b>Fehlerbehebung / Massnahmen</b>	Siehe Kapitel „Kein Logempfang von Cisco Routern“ (Seite 120).
<b>Re-Testing</b>	Der Test wird nicht wiederholt. Siehe Kapitel „Kein Logempfang von Cisco Routern“ (Seite 120).



Tabelle 97: Fehlerprotokoll 1





### 19.31.5 Testabnahme

Sämtliche Tests wurden durch die Testperson (Hetem Shaqiri) durchgeführt. Diese bestätigt mit ihrer Unterschrift, dass die Tests selbständig durchgeführt wurden und die erwarteten Resultate konzeptgemäss erfüllt wurden.

Datum	Name	Unterschrift
23.02.15	Hetem Shaqiri Testperson	
23.02.15	Felix Imobersteg Projektleiter	

**Tabelle 98: Testabnahme**



## 20. Quellenverzeichnis

Betreff	URL	Datum
Archey Installation	<a href="https://debian-blog.org/archey-debian-installation/">https://debian-blog.org/archey-debian-installation/</a>	16.02.15
Backup Script	<a href="https://github.com/prae5/duplicitybackup.sh/blob/master/duplicitybackup.sh">https://github.com/prae5/duplicitybackup.sh/blob/master/duplicitybackup.sh</a>	18.02.15
Black Box Test	<a href="http://de.wikipedia.org/wiki/Black-Box-Test">http://de.wikipedia.org/wiki/Black-Box-Test</a>	24.02.15
Elasticsearch Repositories	<a href="http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/setup-repositories.html">http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/setup-repositories.html</a>	17.02.15
Graylog Installation	<a href="https://www.digitalocean.com/community/tutorials/how-to-install-graylog2-and-centralize-logs-on-ubuntu-14-04">https://www.digitalocean.com/community/tutorials/how-to-install-graylog2-and-centralize-logs-on-ubuntu-14-04</a>	17.02.15
Graylog Installation	<a href="http://docs.graylog.org/en/1.0/pages/installation.html">http://docs.graylog.org/en/1.0/pages/installation.html</a>	17.02.15
Grok-Patterns	<a href="https://github.com/elasticsearch/logstash/blob/v1.1.8/patterns/grok-patterns">https://github.com/elasticsearch/logstash/blob/v1.1.8/patterns/grok-patterns</a>	18.02.15
HERMES 5 IPA	<a href="https://host1.pkorg.ch/download.php?name=KKDok&amp;ndokid=1960">https://host1.pkorg.ch/download.php?name=KKDok&amp;ndokid=1960</a>	09.02.15
Init Scripts	<a href="http://wiki.ubuntuusers.de/Dienste">http://wiki.ubuntuusers.de/Dienste</a>	17.02.15
Logging Allgemein	<a href="http://www.kuehnel.org/bachelor.pdf">http://www.kuehnel.org/bachelor.pdf</a>	24.02.15
Logstash Installation	<a href="https://www.digitalocean.com/community/tutorials/how-to-use-logstash-and-kibana-to-centralize-and-visualize-logs-on-ubuntu-14-04">https://www.digitalocean.com/community/tutorials/how-to-use-logstash-and-kibana-to-centralize-and-visualize-logs-on-ubuntu-14-04</a>	17.02.15
Logstash-Forwarder	<a href="http://antisp.in/2014/03/logstash-forwarder/">http://antisp.in/2014/03/logstash-forwarder/</a>	18.02.15
MongoDB Installation	<a href="http://docs.mongodb.org/manual/tutorial/install-mongodb-on-debian/">http://docs.mongodb.org/manual/tutorial/install-mongodb-on-debian/</a>	17.02.15
VMWare Tools	<a href="http://www.sysadminslife.com/linux/howto-vmware-tools-unter-debian-6-squeeze-und-7-wheezy-installieren/">http://www.sysadminslife.com/linux/howto-vmware-tools-unter-debian-6-squeeze-und-7-wheezy-installieren/</a>	16.02.15
White Box Test	<a href="http://de.wikipedia.org/wiki/White-Box-Test">http://de.wikipedia.org/wiki/White-Box-Test</a>	24.02.15

Tabelle 99: Quellenverzeichnis



## 21. Glossar

Begriff	Bedeutung
Analytic-Engine	Dienst, welcher einem bei der Analyse von Daten unterstützt.
Bare-Metal Virtualisierung	Virtualisierungsstrategie bei welcher ein spezielle Betriebssystem die Virtualisierungsschicht übernimmt
Corporate Design	Erscheinungsbild eines Unternehmens
Corporate Identity	Identität, welche ein Unternehmen vermittelt
Elasticsearch	Flexible, verteilte Echtzeit Such- und Analytic-Engine Dienst
ESX Server	Bare-Metal Hypervisor von VMWare
GELF	Von Graylog verwendetes Protokoll zur Übertragung von Lognachrichten.
Graylog	Open Source Software Sammlung zum Logmanagement
Graylog Server	Softwarekomponente von Graylog welche Logs empfängt, verarbeitet und speichert.
Graylog Web	Webinterface von Graylog, unter welchem gespeicherte Logs angezeigt und durchsucht werden können. Weiter sind Konfigurationsänderungen möglich.
HERMES	Vom Bund entwickelte Projektmethode
Hypervisor	Software oder Betriebssystem, mit welchem Server oder Clients in einer virtuellen Umgebung betrieben werden können.
Icinga	Monitoringsystem (Fork von Nagios)
Latex	Latex ist ein Textsatzungsprogramm, bei welchem der Text und Formatierung in einer speziellen Auszeichnungssprache formuliert wird.
Logstash	Open Source Software welche zur Normalisierung von Logs genutzt wird.
Lumberjack	Von Logstash verwendetes Protokoll zur Übertragung von Lognachrichten.
MongoDB	Dokumentenorientierte NoSQL Datenbank
nginx	Open Source Webserver
REST	Programmierparadigma für verteilte Systeme.
Slack	Messagingservice für Teams
Snapshot	Zustand einer Festplatte, auf welcher zu einem späteren Zeitpunkt zurückgekehrt werden kann
vSphere	Virtualisierungslösung von VMWare
vSphere Center	Verwaltungscenter für mehrere ESX Server
vSphere Client	Software, mit welchem ESX Server und vSphere Center verwaltet werden können

Tabelle 100: Glossar



## 22. Unterschriften für Abnahme


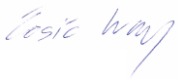
Datum	Name	Unterschrift
27.02.14	Felix Imobersteg Lernender	
27.02.14	Ivan Cosic Fachvorgesetzter	

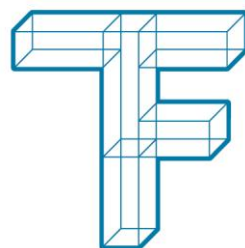
Tabelle 101: Unterschriften für Abnahme



## Teil 3: Anhang

**IPA Projektname:**  
**Autor:**

Zentrales Logmanagement in Betrieb nehmen  
Felix Imobersteg



TECHNISCHE  
FACHSCHULE  
BERN



## 23. Backupkonzept

Server	Pfad	Bemerkung	Tglich (Inkrementell)	Wchentlich (Full)	Monatlich (Full)	Jhrlich (Full)
VMDB1	Datenbank	DB	x	x	x	x
VMDIENST1	D:	DesktopCentral	x	x	x	x
VMDIENST1	E:	WDS	x	x	x	x
VMDIENST1	G:	DATA1	x	x	x	x
VMFSS1	D:	DATA1	x	x	x	x
VMFSL1	D:	DATA1	x	x	x	x
VMFSV1	D:	DATA1	x	x	x	x
VMORGA1	D:	Orgamax	x	x	x	x
VMWEB1	/var/www	Webseiten	x	x	x	x
VMWEB1	Datenbank	MySQL	x	x	x	x

Tabelle 102: Backupkonzept



## 24. Standardinstallation Linux

<b>Hostname</b>	Siehe Namenskonzept
<b>IP-Adresse</b>	Siehe IP Konzept
<b>Gateway</b>	Siehe IP Konzept
<b>Subnetzmaske</b>	Siehe IP Konzept
<b>DNS-Server</b>	86.118.120.170 / 86.118.120.171
<b>OS</b>	Debian Wheezy

Tabelle 103: Angaben Standardinstallation Linux

### 24.1 Step by Step Debian Installation

- Install auswählen
- Language: English
- Country: other - Europe - Switzerland
- Tastatur Layout: Swiss German
- Hostname: Nach dem Namenskonzept zu vergeben
- Domain Name: lwb.ch
- Domain Password: Standard Passwort
- New User: "user"
- Username for your account: user
- Password for user: 1234
- Partitioning method: Guided - use entire disk
- Partitioning scheme: All files in one partition
- Debian archive mirror country: Switzerland
- Debian archive mirror: mirror.switch.ch
- Proxy: without
- Choose software to install: SSH Server
- Install the GRUB boot loader to the MBR: Yes
- restart
- delete "user" -> userdel user



## 25. IP Konzept

### 25.1 Lorraine

VLAN	Netz-ID	Default Gateway	Broadcast	Subnetz-Maske
Verwaltung	86.118.102.0	86.118.102.1	86.118.102.255	255.255.255.0
Lehrer	86.118.104.0	86.118.104.1	86.118.104.255	255.255.255.0
Unterricht	86.118.108.0	86.118.108.1	86.118.109.255	255.255.254.0
VoIP	86.118.112.0	86.118.112.1	86.118.112.255	255.255.255.0
Service	86.118.120.0	86.118.120.1	86.118.120.255	255.255.255.0
Default	10.59.2.0	10.59.2.1	10.59.2.255	255.255.255.0
MGNT	10.163.14.0	10.163.14.1	10.163.14.63	255.255.255.192
ELAN	10.163.14.64	10.163.14.65	10.163.14.127	255.255.255.192

Tabelle 104: Netze Lorraine

### 25.2 Felsenau

VLAN	Netz-ID	Default Gateway	Broadcast	Subnetz-Maske
Verwaltung	86.118.103.0	86.118.103.1	86.118.103.255	255.255.255.0
Lehrer	86.118.105.0	86.118.105.1	86.118.105.255	255.255.255.0
Unterricht	86.118.110.0	86.118.110.1	86.118.111.255	255.255.254.0
VoIP	86.118.114.0	86.118.114.1	86.118.114.255	255.255.255.0
Service	86.118.121.0	86.118.121.1	86.118.121.255	255.255.255.0
Default	10.59.3.0	10.59.3.1	10.59.3.255	255.255.255.0
MGNT	10.163.14.128	10.163.14.129	10.163.14.191	255.255.255.192
ELAN	10.163.14.192	10.163.14.193	10.163.14.255	255.255.255.192

Tabelle 105: Netze Felsenau

### 25.3 Detaillierte Einteilungen Lorraine

#### 25.3.1 Verwaltung

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.102.01	86.118.102.09	9
Clients (DHCP)	86.118.102.10	86.118.102.234	225
Server	86.118.102.235	86.118.102.239	5
Reserve IP's	86.118.102.240	86.118.102.254	15

Tabelle 106: Netz - Verwaltung Lorraine





### 25.3.2 Lehrer

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.104.01	86.118.104.09	9
Clients (DHCP)	86.118.104.10	86.118.104.234	225
Server	86.118.104.235	86.118.104.239	5
Reserve IP's	86.118.104.240	86.118.104.254	15

Tabelle 107: Netz - Lehrer Lorraine

### 25.3.3 Unterricht

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.108.01	86.118.108.09	9
Clients (DHCP)	86.118.108.10	86.118.109.234	481
Server	86.118.109.235	86.118.109.239	5
Reserve IP's	86.118.109.240	86.118.109.254	15

Tabelle 108: Netz - Unterricht Lorraine

### 25.3.4 VoIP

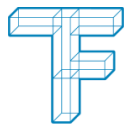
Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.112.01	86.118.112.09	9
Telefonanlage	86.118.112.10	86.118.112.50	41
Clients (DHCP)	86.118.112.51	86.118.112.254	204

Tabelle 109: Netz - VoIP Lorraine

### 25.3.5 Service

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.120.01	86.118.120.09	9
Produktive Server	86.118.120.10	86.118.120.39	30
Diverse Server	86.118.120.40	86.118.120.59	20
Drucker	86.118.120.60	86.118.120.129	70
DNC-Maschinen	86.118.120.130	86.118.120.169	70
Zeit - Terminal	86.118.120.170	86.118.120.189	20
Support Clients	86.118.120.190	86.118.120.209	20
Clients (DHCP)	86.118.120.210	86.118.120.254	45

Tabelle 110: Netz - Service Lorraine



### 25.3.6 Default

Typ	Start IP	End IP	Anzahl
Reserviert BEWAN	10.58.2.1	10.58.2.1.9	9
Netzwerkgeräte	10.58.2.10	10.58.2.39	30
Clients (DHCP)	10.58.2.40	10.58.2.224	184

Tabelle 111: Netz - Default Lorraine

### 25.3.7 MGNT

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	10.163.14.1	10.58.3.9	9
Komponenten	10.163.14.10	10.163.14.62	53

Tabelle 112: Netz - MGNT Lorraine

### 25.3.8 ELAN

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	10.163.14.65	10.58.3.73	9
Komponenten	10.163.14.74	10.163.14.126	53

Tabelle 113: Netz - ELAN Lorraine

## 25.4 Detaillierte Einteilungen Felsenau

### 25.4.1 Verwaltung

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.103.01	86.118.103.09	9
Clients (DHCP)	86.118.103.10	86.118.103.234	225
Reserve IP's	86.118.103.235	86.118.103.254	20

Tabelle 114: Netz - Verwaltung Felsenau



#### 25.4.2 Lehrer

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.105.01	86.118.105.09	9
Clients (DHCP)	86.118.105.10	86.118.105.234	225
Reserve IP's	86.118.105.235	86.118.105.254	20

Tabelle 115 Netz - Lehrer Felsenau

#### 25.4.3 Unterricht

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.110.01	86.118.110.09	9
Clients (DHCP)	86.118.110.10	86.118.111.234	501
Reserve IP's	86.118.111.235	86.118.111.254	20

Tabelle 116 Netz - Unterricht Felsenau

#### 25.4.4 VoIP

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.114.01	86.118.114.09	9
Telefonanlage	86.118.114.10	86.118.114.50	41
Clients (DHCP)	86.118.114.51	86.118.114.254	204

Tabelle 117 Netz - VoIP Felsenau

#### 25.4.5 Service

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	86.118.121.01	86.118.121.09	9
Produktive Server	86.118.121.10	86.118.121.39	30
Diverse Server	86.118.121.40	86.118.121.59	20
Drucker	86.118.121.60	86.118.121.129	70
DNC-Maschinen	86.118.121.130	86.118.121.169	70
Zeit - Terminal	86.118.121.170	86.118.121.189	20
Support Clients	86.118.121.190	86.118.121.209	20
Clients (DHCP)	86.118.121.210	86.118.121.254	45

Tabelle 118 Netz - Service Felsenau



#### 25.4.6 Default

Typ	Start IP	End IP	Anzahl
Reserviert BEWAN	10.58.3.1	10.58.3.9	9
Netzwerkgeräte	10.58.3.10	10.58.3.39	30
Clients (DHCP)	10.58.3.40	10.58.3.124	184

Tabelle 119 Netz - Default Felsenau

#### 25.4.7 MGNT

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	10.163.14.129	10.58.3.137	9
Komponenten	10.163.14.138	10.163.14.190	53

Tabelle 120 Netz - MGNT Felsenau

#### 25.4.8 ELAN

Typ	Start IP	End IP	Anzahl
Netzwerkgeräte	10.163.14.193	10.58.3.201	9
Komponenten	10.163.14.202	10.163.14.254	53

Tabelle 121 Netz - ELAN Felsenau